EIROPAS SAVIENĪBA

EIROPAS PARLAMENTS **PADOME**

Briselē, 2018. gada 28. novembrī
(OR. en)

2016/0409 (COD)
LEX 1849

PE-CONS 36/1/18
REV 1

SIRIS 71
ENFOPOL 337
COPEN 222
SCHENGEN 30
COMIX 335
CODEC 1126

EIROPAS PARLAMENTA UN PADOMES REGULA PAR ŠENGENAS INFORMĀCIJAS SISTĒMAS (*SIS*) IZVEIDI, DARBĪBU UN IZMANTOŠANU POLICIJAS SADARBĪBĀ UN TIESU IESTĀŽU SADARBĪBĀ KRIMINĀLLIETĀS UN AR KO GROZA UN ATCEĻ PADOMES LĒMUMU 2007/533/TI UN ATCEĻ EIROPAS PARLAMENTA UN PADOMES REGULU (EK) Nr. 1986/2006 UN KOMISIJAS LĒMUMU 2010/261/ES

EIROPAS PARLAMENTA UN PADOMES
REGULA (ES) 2018/...

(2018. gada 28. novembris)

par Šengenas Informācijas sistēmas (*SIS*)
izveidi, darbību un izmantošanu
policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās
un ar ko groza un atceļ Padomes Lēmumu 2007/533/TI
un atceļ Eiropas Parlamenta un Padomes
Regulu (EK) Nr. 1986/2006
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 otrās 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[1],

[1] Eiropas Parlamenta 2018. gada 24. oktobra nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2018. gada 19. novembra lēmums.

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 Savienības brīvības, drošības un tiesiskuma telpā, atbalstot valsts kompetento iestāžu jo īpaši robežsardzes, policijas, muitas dienestu, imigrācijas iestāžu un iestāžu, kas atbildīgas par noziedzīgu nodarījumu novēršanu, atklāšanu, izmeklēšanu vai saukšanu pie atbildības par tiem, vai kriminālsodu izpildi, operatīvo sadarbību.

(2) *SIS* sākotnēji 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[1] (Konvencija, ar ko īsteno Šengenas nolīgumu). Otrās paaudzes *SIS* (*SIS II*) izveide tika uzticēta Komisijai, ievērojot Padomes Regulu (EK) Nr. 2424/2001[2] un Padomes Lēmumu 2001/886/TI[3].To vēlāk izveidoja ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1987/2006[4] un ar Padomes Lēmumu 2007/533/TI[5]. *SIS II* aizstāja *SIS*, kas bija izveidota, ievērojot Konvenciju, ar ko īsteno Šengenas nolīgumu.

---

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

2 Padomes Regula (EK) Nr. 2424/2001 (2001. gada 6. decembris) par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izstrādi (OV L 328, 13.12.2001., 4. lpp.).

3 Padomes Lēmums 2001/886/TI (2001. gada 6. decembris) par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izstrādi (OV L 328, 13.12.2001., 4. lpp.).

4 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 381, 28.12.2006., 4. lpp.).

5 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.).

(3) Trīs gadus pēc *SIS II* darbības sākšanas Komisija veica sistēmas novērtējumu saskaņā ar Regulu (EK) Nr. 1987/2006 un Lēmumu 2007/533/TI. Komisija 2016. gada 21. decembrī Eiropas Parlamentam un Padomei iesniedza Otrās paaudzes Šengenas Informācijas Sistēmas (*SIS II*) novērtējuma ziņojumu saskaņā ar Regulas (EK) Nr. 1987/2006 24. panta 5. punktu, 43. panta 3. punktu un 50. panta 5. punktu un Lēmuma 2007/533/TI 59. panta 3. punktu un 66. panta 5. punktu un saistīto dienestu darba dokumentu. Ieteikumi, kas izklāstīti minētajos dokumentos, attiecīgos gadījumos būtu jāatspoguļo šajā regulā.

(4) Šī regula ir *SIS* juridiskais pamats attiecībā uz jautājumiem, uz ko attiecas Līguma par Eiropas Savienības darbību (LESD) Trešās daļas V sadaļas 4. un 5. nodaļa. Eiropas Parlamenta un Padomes Regula (ES) 2018/...[1+] ir *SIS* juridiskais pamats attiecībā uz jautājumiem, uz ko attiecas LESD Trešās daļas V sadaļas 2. nodaļa.

---

[1] Eiropas Parlamenta un Padomes Regula (ES) 2018/... (... gada ...) par Šengenas Informācijas sistēmas (*SIS*) izveidi, darbību un izmantošanu robežpārbaužu jomā un ar kuru groza Konvenciju, ar ko īsteno Šengenas nolīgumu, un groza un atceļ Regulu (EK) Nr. 1987/2006 (OV L ...).

[+] OV: lūgums tekstā ievietot numuru un papildināt zemsvītras piezīmē ietverto publikācijas atsauci dokumentā PE-CONS 35/18 iekļautajai regulai.

(5) Tas, ka *SIS* juridisko pamatu veido atsevišķi instrumenti, neskar principu, ka *SIS* ir vienota informācijas sistēma, kurai kā tādai būtu jādarbojas. Tai būtu jāietver valsts struktūru, sauktu par *SIRENE* birojiem, vienots tīkls papildinformācijas apmaiņas nodrošināšanai. Tāpēc dažiem minēto instrumentu noteikumiem vajadzētu būt identiskiem.

(6) Ir jāprecizē *SIS* mērķi, tās tehniskās uzbūves daži elementi un finansējums, jāparedz noteikumi par tās darbību no viena gala līdz otram un izmantošanu un jādefinē pienākumi. Ir arī jānosaka sistēmā ievadāmo datu kategorijas, datu ievadīšanas un apstrādes mērķi un ievadīšanas kritēriji. Ir arī vajadzīgi noteikumi, kas reglamentētu brīdinājumu dzēšanu, iestādes, kas ir pilnvarotas piekļūt datiem, biometrisko datu izmantošanu un sīkāk noteiktu datu aizsardzības un datu apstrādes noteikumus.

(7) Brīdinājumi *SIS* ietver tikai to informāciju, kas nepieciešama personas vai priekšmeta identifikācijai un veicamajai darbībai. Tādēļ dalībvalstīm vajadzības gadījumā būtu jāapmainās ar papildinformāciju, kas saistīta ar brīdinājumiem.

(8) *SIS* sastāv no centrālās sistēmas (centrālā *SIS*) un valstu sistēmām. Valstu sistēmās varētu būt pilnīga vai daļēja *SIS* datubāzes kopija, ko var kopīgot divas vai vairāk dalībvalstis. Ņemot vērā to, ka *SIS* ir vissvarīgākais informācijas apmaiņas rīks Eiropā drošības un efektīvas robežu pārvaldības nodrošināšanai, ir jānodrošina tās nepārtraukta darbība gan centrālajā, gan valstu līmenī. *SIS* pieejamība būtu stingri jāuzrauga centrālā un dalībvalstu līmenī, un visi incidenti, kad tā nav bijusi pieejama galalietotājiem, būtu jāreģistrē un par tiem būtu jāziņo ieinteresētajām personām valsts un Savienības līmenī. Katrai dalībvalstij būtu jāizveido rezerves sistēma savai valsts sistēmai. Dalībvalstīm būtu arī jānodrošina nepārtraukta savienojamība ar centrālo *SIS*, šajā nolūkā tām vajadzētu būt dublētiem, fiziski un ģeogrāfiski nodalītiem savienojuma punktiem. Centrālā *SIS* un komunikācijas infrastruktūra būtu jāekspluatē tā, lai to darbība tiktu nodrošināta 24 stundas diennaktī, 7 dienas nedēļā. Lai to panāktu, Eiropas Savienības Aģentūrai lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā ("*eu-LISA*"), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/...[1+], balstoties uz neatkarīgu ietekmes novērtējumu un izmaksu un ieguvumu analīzi, būtu jāīsteno tehniski risinājumi ar mērķi pastiprināt *SIS* nepārtrauktu pieejamību.

---

[1] Eiropas Parlamenta un Padomes Regula (ES) 2018/... (... gada ...) par Eiropas Savienības Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*), un ar ko groza Regulu (EK) Nr. 1987/2006 un Padomes Lēmumu 2007/533/TI un atceļ Regulu (ES) Nr. 1077/2011 (OV L …).

[+] OV: lūgums tekstā ievietot numuru un papildināt zemsvītras piezīmē ietverto publikācijas atsauci dokumentā PE-CONS 29/18 iekļautajai regulai.

(9) Ir jāuztur rokasgrāmata ar sīki izstrādātiem noteikumiem par papildinformācijas apmaiņu attiecībā uz to, kādas darbības jāveic brīdinājuma gadījumā ("*SIRENE* rokasgrāmata"). *SIRENE* birojiem būtu jānodrošina ātra un efektīva šādas informācijas apmaiņa.

(10) Lai nodrošinātu efektīvu apmaiņu ar papildinformāciju, tostarp par veicamo darbību konkrēta brīdinājuma gadījumā, ir lietderīgi stiprināt *SIRENE* biroju darbību, precizējot prasības attiecībā uz pieejamajiem resursiem un lietotāju apmācību un reakcijas laiku uz jautājumiem, ko tie saņem no citiem *SIRENE* birojiem.

(11) Dalībvalstīm būtu jānodrošina, lai to *SIRENE* biroja darbiniekiem būtu savu uzdevumu veikšanai vajadzīgās valodu prasmes un attiecīgo tiesību aktu un procesuālo normu zināšanas.

(12) Lai varētu pilnībā izmantot *SIS* iespējas, dalībvalstīm būtu jānodrošina, ka galalietotāji un *SIRENE* biroju darbinieki regulāri apmeklē mācības, tostarp attiecībā uz datu drošību, datu aizsardzību un datu kvalitāti. *SIRENE* birojiem vajadzētu būt iesaistītiem apmācību programmu izstrādē. Cik vien iespējams, *SIRENE* birojiem vajadzētu arī paredzēt savstarpēju darbinieku apmaiņu vismaz reizi gadā. Dalībvalstis tiek aicinātas veikt atbilstošus pasākumus, lai izvairītos no kvalifikācijas un pieredzes zaudēšanas darbinieku mainības dēļ.

(13) *SIS* centrālo komponentu darbības pārvaldību īsteno *eu-LISA*. Lai *eu-LISA* varētu piešķirt nepieciešamos finanšu resursus un personālu, kas aptvertu visus centrālās *SIS* un komunikācijas infrastruktūras darbības pārvaldības aspektus, šajā regulā būtu detalizēti jāizklāsta *eu-LISA* uzdevumi, jo īpaši attiecībā uz papildinformācijas apmaiņas tehniskajiem aspektiem.

(14) Neskarot dalībvalstu atbildību par *SIS* ievadīto datu precizitāti un *SIRENE* biroju kā kvalitātes koordinatoru lomu, *eu-LISA* vajadzētu būt atbildīgai par datu kvalitātes uzlabošanu, ieviešot centrālu datu kvalitātes uzraudzības instrumentu, un būtu jāsniedz regulāri ziņojumi Komisijai un dalībvalstīm. Komisijai būtu jāziņo Eiropas Parlamentam un Padomei par datu kvalitātes jautājumiem, kas radušies. Lai vēl vairāk uzlabotu *SIS* datu kvalitāti, *eu-LISA* arī būtu valstu apmācības struktūrām un, ciktāl iespējams, *SIRENE* birojiem un galalietotājiem jāpiedāvā apmācība par *SIS* izmantošanu.

(15) Lai varētu labāk uzraudzīt *SIS* izmantošanu un analizēt noziedzīgu nodarījumu tendences, *eu-LISA* spējām sniegt dalībvalstīm, Eiropas Parlamentam, Padomei, Komisijai, Eiropolam, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūrai statistikas ziņojumus būtu jāatbilst jaunākajam tehnikas līmenim, neietekmējot datu integritāti. Tādēļ būtu jāizveido centrālais repozitorijs. Minētajā repozitorijā saglabātajā vai no tā iegūtajā statistikā nebūtu jāietver nekādi personas dati. Dalībvalstīm atbilstīgi sadarbības mehānismam starp uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju saskaņā ar šo regulu būtu jāpaziņo statistika par tiesību uz piekļuvi izmantošanu, neprecīzu datu labošanu un nelikumīgi glabātu datu dzēšanu.

(16) *SIS* būtu jāiekļauj jaunas datu kategorijas, kas ļauj galalietotājiem, pamatojoties uz brīdinājumu un nezaudējot laiku, pieņemt uz informāciju balstītus lēmumus. Tādēļ, lai atvieglotu identifikāciju un atklātu personas, kas izmanto vairākas identitātes, brīdinājumā būtu jāiekļauj arī atsauce uz attiecīgās personas personas identifikācijas dokumentu vai tā numuru, ja šāda informācija ir pieejama, un dokumenta kopija, ja iespējams – krāsu kopija.

(17) Kompetentajām iestādēm vajadzētu spēt, kad tas noteikti ir nepieciešams, ievadīt *SIS* specifisku informāciju, kas saistīta ar kādu personas īpašu, objektīvu un fizisku pazīmi, kura nevar mainīties, piemēram, tetovējumiem, zīmēm vai rētām.

(18) Veidojot brīdinājumu, būtu jāiekļauj visi attiecīgie dati, ja tie ir pieejami, jo īpaši attiecīgās personas vārds, lai līdz minimumam samazinātu informācijas viltus atbilsmju risku un nevajadzīgas operatīvās darbības.

(19) *SIS* nebūtu jāglabā nekādi dati, kas izmantoti meklēšanā, izņemot reģistra ierakstu glabāšanu, lai pārbaudītu, vai meklēšana ir likumīga, lai uzraudzītu datu apstrādes likumību, veiktu pašuzraudzību un nodrošinātu valsts sistēmu pareizu darbību, kā arī datu integritāti un drošību.

(20) *SIS* vajadzētu būt iespējai apstrādāt biometriskos datus, lai palīdzētu ticami identificēt attiecīgās personas. Jebkādai fotogrāfiju, sejas attēlu vai daktiloskopisko datu ievadīšanai *SIS* un jebkādai šādu datu izmantošanai nebūtu jāpārsniedz tas, kas ir nepieciešams izvirzītajiem mērķiem, šādas darbības būtu jāatļauj ar Savienības tiesību aktiem, tām būtu jānotiek, ievērojot pamattiesības, tostarp bērna intereses, un tām vajadzētu būt saskaņā ar Savienības tiesību aktiem datu aizsardzības jomā, tostarp attiecīgajiem datu aizsardzības noteikumiem, kas noteikti šajā regulā. Tādā pašā sakarā, lai novērstu nepareizas identifikācijas dēļ radušās grūtības, *SIS* vajadzētu būt arī iespējai apstrādāt to personu datus, kuru identitāte ir ļaunprātīgi izmantota, ievērojot attiecīgus aizsardzības pasākumus, saņemot attiecīgās personas piekrišanu attiecībā uz katru datu kategoriju, jo īpaši plaukstu nospiedumiem, un stingri ierobezojot mērķus, kuriem šādus personas datus var likumīgi apstrādāt.

(21) 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*, ievērojot principus, kas noteikti 4. pantā Eiropas Parlamenta un Padomes Direktīvā (ES) 2016/68[1] un 5. pantā Eiropas Parlamenta un Padomes Regulā (ES) 2016/679[2]. Tam būtu jānodrošina, ka *SIS* darbojas kā galvenais papildu pasākums zonā bez iekšējās robežkontroles un labāk risina noziedzības un noziedznieku mobilitātes pārrobežu aspektu.

(22) Šajā regulā būtu jāparedz daktiloskopisko datu, fotogrāfiju un sejas attēlu izmantošanas nosacījumi identifikācijas un pārbaudes nolūkiem. Sejas attēli un fotogrāfijas identifikācijas nolūkā sākumā būtu jāizmanto tikai saistībā ar regulārajām robežšķērsošanas vietām. Šādai izmantošanai būtu jānotiek, ievērojot Komisijas ziņojumu, kurā apstiprina tehnoloģijas pieejamību, uzticamību un to, vai tā spēj pareizi darboties.

---

[1] 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., 89. lpp.).

[2] 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.).

(23) Automatizēta pirkstu nospiedumu identifikācijas pakalpojuma ieviešana *SIS* papildina esošo Prīmes mehānismu savstarpējai pārrobežu tiešsaistes piekļuvei valstu DNS datubāzēm un automatizētajām pirkstu nospiedumu identifikācijas sistēmām, kā izklāstīts Padomes Lēmumā 2008/615/TI[1] un 2008/616/TI[2]. *SIS* daktiloskopisko datu meklēšana pieļauj izdarītāja aktīvu meklēšanu. Tādēļ būtu jāparedz iespēja augšupielādēt *SIS* nezināma izdarītāja daktiloskopiskos datus, ar noteikumu, ka minēto datu īpašnieku var identificēt ar ļoti augstu varbūtības pakāpi kā personu, kas izdarījusi smagu noziegumu vai terorisma aktu. Tas jo īpaši attiecas uz gadījumu, kad daktiloskopiskos datus atrod uz ieroča vai jebkura cita objekta, kas izmantots nodarījumā. Vienkārša daktiloskopisko datu atrašanās nozieguma vietā nebūtu jāuzskata par norādi uz ļoti augstu varbūtības pakāpi, ka konkrētie daktiloskopiskie dati ir izdarītāja daktiloskopiskie dati. Vēl viens priekšnoteikums, lai izveidotu šādu brīdinājumu, būtu, ka aizdomās turētā identitāti nevar noteikt, izmantojot jebkuru citu attiecīgu valsts, Savienības vai starptautisko datubāzi. Ja daktiloskopisko datu meklēšana noved pie iespējamas atbilstības, dalībvalstij būtu jāveic turpmākas pārbaudes, iesaistot arī ekspertus, lai noteiktu, vai aizdomās turētais ir *SIS* saglabāto pirkstu nospiedumu īpašnieks, un būtu jānoskaidro personas identitāte. Procedūra būtu jāpiemēro saskaņā ar valsts tiesību aktiem. Šāda identifikācija varētu būtiski palīdzēt izmeklēšanā un varētu novest līdz apcietināšanai ar noteikumu, ka visi apcietināšanas nosacījumi ir izpildīti.

---

1 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.).

2 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.).

(24) Būtu jāatļauj meklēt daktiloskopiskos datus, kas glabājas *SIS*, ar pilniem vai nepilniem pirkstu nospiedumu vai plaukstu nospiedumu komplektiem, kas atrasti noziedzīga nodarījuma izdarīšanas vietā, ja tiek konstatēta augsta varbūtības pakāpe, ka tie ir smaga nozieguma vai teroristu nodarījuma izdarītāja pirkstu nospiedumi, ar noteikumu, ka meklēšana tiek vienlaikus veikta attiecīgajās valstu pirkstu nospiedumu datubāzēs. Īpaša uzmanība būtu jāpievērš to kvalitātes standartu izveidei, kuri piemērojami biometrisko datu, tostarp latentu daktiloskopisko datu, glabāšanai.

(25) Ja personas identitāti nevar noskaidrot, izmantojot citus līdzekļus, būtu jāizmanto daktiloskopiskie dati, lai mēģinātu identificēt personu. Visos gadījumos būtu jāatļauj identificēt personu, izmantojot daktiloskopiskos datus.

(26) Skaidri definētos gadījumos, kad daktiloskopiskie dati nav pieejami, vajadzētu būt iespējai brīdinājumam pievienot DNS profilu. Minētajam DNS profilam vajadzētu būt pieejamam tikai pilnvarotiem lietotājiem. DNS profiliem būtu jāatvieglo tādu pazudušu personu identifikācija, kurām vajadzīga aizsardzība, jo īpaši pazudušu bērnu identifikācija, tostarp, atļaujot identifikācijai izmantot tiešo augšupējo radinieku, pēcnācēju vai brāļu un māsu DNS profilus. DNS datos būtu jāietver tikai minimālā informācija, kas nepieciešama pazudušās personas identifikācijai.

(27) DNS profili no *SIS* būtu jāizgūst tikai tad, ja identificēšana ir vajadzīga un samērīga šajā regulā noteiktajos nolūkos. DNS profili būtu jāizgūst vai jāapstrādā tikai tiem mērķiem, kuriem tie ievadīti *SIS*. Būtu jāpiemēro šajā regulā noteiktie datu aizsardzības un drošības noteikumi. Vajadzības gadījumā būtu jāievieš papildu aizsardzības pasākumi, kad tiek izmantoti DNS profili, lai izvairītos no jebkāda riska, kas saistīts ar kļūdainām atbilsmēm, uzlaušanu un neatļautu kopīgošanu ar trešām personām.

(28) *SIS* būtu jāietver brīdinājumi par personām, kuras meklē apcietināšanai nolūkā tās nodot vai izdot. Papildus brīdinājumiem ir lietderīgi paredzēt tādas papildinformācijas apmaiņu ar *SIRENE* biroju starpniecību, kas nepieciešama nodošanas un izdošanas procedūrās. *SIS* jo īpaši būtu jāapstrādā dati, kas minēti Padomes Pamatlēmuma 2002/584/TI[1] 8. pantā. Operatīvu iemeslu dēļ ir lietderīgi, ka izdevēja dalībvalsts esošo brīdinājumu par apcietināšanu uz laiku padara nepieejamu, ja ir saņemta tiesu iestāžu 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 principā nebūtu jāpārsniedz 48 stundas.

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

---

[1] 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.).

(30) *SIS* vajadzētu būt ietvertiem brīdinājumiem par pazudušām personām vai par neaizsargātām personām, kam jāliedz ceļot, lai nodrošinātu šo personu aizsardzību vai novērstu sabiedriskās drošības vai sabiedriskās kārtības apdraudējumus. Attiecībā uz bērniem šiem brīdinājumiem un attiecīgajām procedūrām būtu jākalpo bērna interesēm saskaņā ar Eiropas Savienības Pamattiesību hartas 24. pantu un Apvienoto Nāciju Organizācijas 1989. gada 20. novembra Konvencijas par bērna tiesībām 3. pantu. Kompetento iestāžu, tostarp tiesu iestāžu, darbības un lēmumi pēc brīdinājuma par bērnu būtu jāveic un jāpieņem sadarbībā ar bērnu aizsardzības iestādēm. Vajadzības gadījumā būtu jāinformē arī valsts palīdzības dienests pazudušu bērnu meklēšanai.

(31) Pēc kompetentās iestādes lūguma būtu jāievada brīdinājumi par pazudušām personām, kas jāaizsargā. Par visiem bērniem, kuri ir pazuduši no dalībvalstu uzņemšanas vietām, *SIS* būtu jāievada brīdinājums par pazudušām personām.

(32) Brīdinājumi par vecāku veiktas nolaupīšanas riskam pakļautiem bērniem būtu jāievada *SIS* pēc kompetento iestāžu – tostarp tiesu iestāžu, kurām saskaņā ar valsts tiesību aktiem ir jurisdikcija lietās par vecāku atbildību, – lūguma. Brīdinājums *SIS* par vecāku veiktas nolaupīšanas riskam pakļautiem bērniem būtu jāievada tikai tad, ja pastāv konkrēts un acīmredzams risks, un ierobežotos apstākļos. Tādēļ ir jāparedz stingri un piemēroti aizsardzības pasākumi. Kompetentajai iestādei būtu jāņem vērā bērna personīgie apstākļi un vide, kurā bērns atrodas, kad tā novērtē, vai pastāv konkrēts un acīmredzams risks, ka bērns var tikt nenovēršami un nelikumīgi izvests no dalībvalsts.

(33) Šajā regulā būtu jāizveido jauna brīdinājumu kategorija attiecībā uz dažām neaizsargātu personu kategorijām, kam jāliedz ceļot. Personas, kurām vecuma, invaliditātes vai ģimenes apstākļu dēļ ir vajadzīga aizsardzība, būtu jāuzskata par neaizsargātām personām.

(34) Brīdinājumi par bērniem, kam jāliedz ceļot viņu pašu aizsardzības dēļ, būtu jāievada *SIS*, ja pastāv konkrēts un acīmredzams risks, ka bērnus var aizvest no dalībvalsts teritorijas vai viņi var to atstāt. Šādi brīdinājumi būtu jāievada, ja ceļojums tiem radītu risku kļūt par cietušajiem cilvēku tirdzniecībā vai saistībā ar piespiedu laulību, sieviešu dzimumorgānu kropļošanu vai citādu ar dzimumu saistītu vardarbību, vai kļūt par cietušajiem vai tikt iesaistītiem teroristu nodarījumos, to, ka viņus iesauks vai iesaistīs bruņotās grupās vai viņiem liks aktīvi piedalīties karadarbībā.

(35) Brīdinājumi par neaizsargātām personām, kam jāliedz ceļot viņu pašu aizsardzības dēļ, būtu jāievada, ja ceļojums tiem radītu risku kļūt par cietušajiem cilvēku tirdzniecībā vai ar dzimumu saistītā vardarbībā.

(36) Lai nodrošinātu stingrus un piemērotus aizsardzības pasākumus, brīdinājumi par bērniem vai citām neaizsargātām personām, kam jāliedz ceļot, būtu – ja tas prasīts valsts tiesību aktos – jāievada *SIS* pēc tiesu iestādes lēmuma vai kompetentas iestādes lēmuma, ko apstiprinājusi tiesu iestāde.

(37) Jauna veicamā darbība būtu jāievada, lai ļautu attiecīgo personu apturēt un nopratināt ar mērķi izdevējai dalībvalstij iegūt izsmeļošu informāciju. Šī darbība būtu jāpiemēro gadījumos, kad, pamatojoties uz skaidru norādi, pastāv aizdomas, ka persona plāno izdarīt vai ir izdarījusi kādu no nodarījumiem, kas minēti Pamatlēmuma 2002/584/TI 2. panta 1. un 2. punktā, ja ir vajadzīga papildu informācija, lai izpildītu brīvības atņemšanas sodu vai ar brīvības atņemšanu saistītu drošības līdzekli personai, kas ir notiesāta par kādu no Pamatlēmuma 2002/584/TI 2. panta 1. un 2. punktā minētajiem nodarījumiem, vai ja ir pamats uzskatīt, ka viņš vai viņa izdarīs kādu no minētajiem nodarījumiem. Šai veicamajai darbībai arī nebūtu jāskar esošie savstarpējas tiesiskās palīdzības mehānismi. Tai būtu jāsniedz pietiekama informācija, lai lemtu par turpmākajām darbībām. Šai jaunajai darbībai nebūtu jāizvēršas par personas meklēšanu vai tās apcietināšanu. Būtu jāsaglabā aizdomās turēto un apsūdzēto personu procesuālās tiesības saskaņā ar Savienības un valstu tiesību aktiem, tostarp viņu tiesības uz advokāta palīdzību saskaņā ar Eiropa Parlamenta un Padomes Direktīvu 2013/48/EK[1].

(38) Brīdinājumu gadījumā par priekšmetiem izņemšanai vai izmantošanai par pierādījumiem kriminālprocesā attiecīgie priekšmeti būtu jāizņem saskaņā ar valsts tiesību aktiem, kas nosaka, vai un saskaņā ar kādiem nosacījumiem priekšmets ir jāizņem, jo īpaši tad, ja tas ir pie tā likumīgā īpašnieka.

---

[1] Eiropas Parlamenta un Padomes Direktīva 2013/48/ES (2013. gada 22. oktobris) par tiesībām uz advokāta palīdzību kriminālprocesā un Eiropas apcietināšanas ordera procesā, par tiesībām uz to, ka pēc brīvības atņemšanas informē trešo personu, un par tiesībām, kamēr atņemta brīvība, sazināties ar trešām personām un konsulārajām iestādēm (OV L 294, 6.11.2013., 1. lpp.).

(39) *SIS* būtu jāiekļauj jaunas kategorijas priekšmetiem ar augstu vērtību, piemēram, informācijas tehnoloģiju vienības, kuras var identificēt un meklēt ar unikālu identifikācijas numuru.

(40) Attiecībā uz brīdinājumiem, kas *SIS* ievadīti par dokumentiem izņemšanai vai izmantošanai par pierādījumiem kriminālprocesā, termins "neīsts" būtu jāinterpretē kā tāds, kas aptver gan falsificētus, gan viltotus dokumentus.

(41) Dalībvalstīm vajadzētu būt iespējai brīdinājumam pievienot norādi, ko sauc par atzīmi un kurā norāda, ka saskaņā ar brīdinājumu veicamā darbība netiks veikta tās teritorijā. Ja brīdinājumus ievada apcietināšanai nodošanas nolūkā, nekas šajā regulā nebūtu jāinterpretē kā atkāpe no Pamatlēmuma 2002/584/TI noteikumiem vai liegums tos piemērot. Lēmums brīdinājumam pievienot atzīmi nolūkā neizpildīt Eiropas apcietināšanas orderi būtu jāpamato vienīgi ar minētajā pamatlēmumā paredzētajiem atteikuma iemesliem.

(42) Ja brīdinājumam pievienota atzīme un ja kļūst zināma tās personas atrašanās vieta, ko meklē, lai apcietinātu nolūkā to nodot, tad personas atrašanās vieta vienmēr būtu jāpaziņo izdevējai tiesu iestādei, kas var pieņemt lēmumu pārsūtīt Eiropas apcietināšanas orderi kompetentajai tiesu iestādei saskaņā ar Pamatlēmuma 2002/584/TI noteikumiem.

(43) Dalībvalstīm vajadzētu būt iespējai veikt brīdinājumu sasaisti *SIS*. Tam, ka tiek izveidotas saites starp diviem vai vairāk brīdinājumiem, nevajadzētu ietekmēt veicamo darbību, brīdinājumu pārskatīšanas periodu vai piekļuves tiesības brīdinājumiem.

(44) Brīdinājumi *SIS* nebūtu jāglabā ilgāk kā nepieciešams, lai īstenotu konkrētos mērķus, kuriem tie ievadīti. Dažādu kategoriju brīdinājumu pārskatīšanas periodiem vajadzētu būt piemērotiem to nolūkiem. Brīdinājumi par priekšmetiem, kas ir saistīti ar brīdinājumu par personām, būtu jāsaglabā tikai tik ilgi, kamēr tiek saglabāts brīdinājums par personu. Lēmumiem saglabāt brīdinājumus par personām būtu jābalstās uz visaptverošu individuālu izvērtējumu. Dalībvalstīm būtu jāpārskata brīdinājumi par personām un priekšmetiem paredzētajos pārskatīšanas periodos un būtu jāglabā statistika par to brīdinājumu skaitu, kuru saglabāšanas periods ir pagarināts.

(45) Brīdinājuma ievadīšanai *SIS* un brīdinājuma *SIS* beigu termiņa pagarināšanai būtu jāpiemēro samērīguma prasība, kas ietver izvērtējumu par to, vai konkrētais gadījums ir atbilstīgs, piemērots un pietiekami svarīgs, lai brīdinājumu iekļautu *SIS*. Attiecībā uz teroristu nodarījumiem gadījums būtu jāuzskata par atbilstīgu, piemērotu un pietiekami svarīgu, lai būtu brīdinājums *SIS*. Sabiedriskās vai valsts drošības iemeslu dēļ dalībvalstīm būtu jāatļauj izņēmuma kārtā atturēties ievadīt brīdinājumu *SIS*, ja ir iespējams, ka tas varētu traucēt oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras.

(46) Ir jāparedz noteikumi par brīdinājumu dzēšanu. Brīdinājums būtu jāglabā tikai tik ilgi, cik vajadzīgs, lai sasniegtu mērķi, kādam tas ievadīts. Ņemot vērā dalībvalstu atšķirīgo praksi tā laika noteikšanā, kad brīdinājums ir izpildījis savu mērķi, ir lietderīgi katrai brīdinājumu kategorijai noteikt sīki izstrādātus kritērijus, lai varētu noteikt, kad tas būtu jādzēš.

(47) *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, vajadzētu būt saistošām šajā regulā noteiktajām drošības prasībām un uz tām būtu jāattiecina vienota procedūra ziņošanai par incidentiem. To darbiniekiem vajadzētu būt pienācīgi apmācītiem un informētiem par jebkādiem nodarījumiem un sankcijām šajā sakarā.

(48) Datus, kas apstrādāti *SIS*, un saistīto papildinformāciju, ar kuru notikusi apmaiņa, ievērojot šo regulu, nevajadzētu nosūtīt vai darīt pieejamus trešām valstīm vai starptautiskām organizācijām.

(49) Ir lietderīgi piešķirt piekļuvi *SIS* dienestiem, kas atbildīgi par transportlīdzekļu, laivu un gaisa kuģu reģistrāciju, lai tie varētu pārbaudīt, vai attiecīgo satiksmes līdzekli dalībvalstīs meklē, lai izņemtu. Ir lietderīgi piešķirt piekļuvi *SIS* arī dienestiem, kas atbildīgi par šaujamieroču reģistrāciju, lai tie varētu pārbaudīt, vai attiecīgo šaujamieroci dalībvalstīs meklē, lai izņemtu, vai pārbaudīt, vai par personu, kas prasa reģistrāciju, ir brīdinājums.

(50) Tieša piekļuve *SIS* būtu jāpiešķir tikai kompetentiem valdības dienestiem. Piekļuve būtu jāattiecina tikai uz brīdinājumiem par attiecīgajiem satiksmes līdzekļiem un to reģistrācijas dokumentiem vai numura zīmēm, vai šaujamieročiem un personām, kas prasa reģistrāciju. Šādiem dienestiem būtu policijas iestādēm jāziņo par jebkuru informācijas atbilsmi *SIS*, kam būtu jāveic turpmāka rīcība saskaņā ar konkrēto brīdinājumu *SIS* un ar *SIRENE* biroju starpniecību par informācijas atbilsmi jāpaziņo izdevējai dalībvalstij.

(51) Neskarot šajā regulā paredzētus specifiskākus noteikumus, personas datu apstrādei – tostarp to vākšanai un paziņošanai –, ko valsts kompetentās iestādes saskaņā ar šo regulu veic teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, atklāšanas, izmeklēšanas nolūkos vai lai sauktu pie atbildības par tiem, vai lai izpildītu krimināsodus, būtu jāpiemēro valstu normatīvie un administratīvie akti, kas pieņemti, ievērojot Direktīvu (ES) 2016/680. Uz piekļuvi *SIS* ievadītajiem datiem un uz tiesībām šādus datus meklēt, kas dotas valstu kompetentajām iestādēm, kuras ir atbildīgas par teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu, izmeklēšanu vai saukšanu pie atbildības par tiem vai par krimināsodu izpildi, ir attiecināmi visi attiecīgi noteikumi, kas paredzēti šajā regulā un Direktīvā (ES) 2016/680, kā tā transponēta valsts tiesību aktos, un jo īpaši uzraudzība, ko veic Direktīvā (ES) 2016/680 minētās uzraudzības iestādes.

(52) Neskarot šajā regulā paredzētus specifiskākus noteikumus par personas datu apstrādi, personas datu apstrādei, ko dalībvalstis veic saskaņā ar šo regulu, būtu jāpiemēro Regula (ES) 2016/679, ja vien šādu apstrādi valsts kompetentās iestādes neveic teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas nolūkos vai lai sauktu pie atbildības par tiem.

(53) Personas datu apstrādei, ko veic Savienības iestādes un struktūras, pildot savus pienākumus saskaņā ar šo regulu, būtu jāpiemēro Eiropas Parlamenta un Padomes Regula (ES) 2018/...[1+].

(54) Personas datu apstrādei, ko veic Eiropols saskaņā ar šo regulu, būtu jāpiemēro Eiropas Parlamenta un Padomes Regula (ES) 2016/794[2].

(55) Ja meklēšanā, ko *SIS* veic *Eurojust* valstu locekļi un to palīgi, tiek konstatēts dalībvalsts ievadīts brīdinājums, *Eurojust* nevar veikt prasīto darbību. Tādēļ tai būtu jāinformē attiecīgā dalībvalsts, kas ļautu tai izskatīt konkrēto gadījumu.

---

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

\+ OV: lūgums tekstā ievietot numuru un zemsvītras piezīmē aizpildīt publikācijas informāciju dokumentā PE-CONS 31/18 iekļautajai regulai.

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

(56) Lietojot *SIS*, kompetentajām iestādēm būtu jānodrošina, ka tiek ievērota tās personas cieņa un integritāte, kuras datus apstrādā. Personas datu apstrāde, ko veic šīs regulas vajadzībām, nedrīkst diskriminēt personas jebkādu tādu iemeslu dēļ kā dzimums, rase vai etniskā izcelsme, reliģija vai pārliecība, invaliditāte, vecums vai seksuālā orientācija.

(57) 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 kārtības noteikumi, kas paredzēti Padomes Regulā (EEK, *Euratom*, EOTK) Nr. 259/68[1] ("Civildienesta noteikumi").

(58) Gan dalībvalstīm, gan *eu-LISA* būtu jāizstrādā drošības plāns, lai atvieglinātu saistību izpildi drošības jomā, un tām būtu jāsadarbojas, lai no kopīga skatu punkta risinātu drošības jautājumus.

[1] OV L 56, 4.3.1968., 1. lpp.

(59) Neatkarīgām valsts uzraudzības iestādēm, kas minētas Regulā (ES) 2016/679 un Direktīvā (ES) 2016/680 ("uzraudzības iestādes"), būtu jāuzrauga personas datu apstrādes, ko dalībvalstis veic saskaņā ar šo regulu, tostarp papildinformācijas apmaiņas, likumība. Uzraudzības iestādēm būtu jāpiešķir pietiekami resursi šā uzdevuma veikšanai. Būtu jāparedz datu subjektu tiesības uz piekļuvi saviem personas datiem, kas glabājas *SIS*, to labošanu un dzēšanu, un visi turpmāki tiesiskās aizsardzības līdzekļi valsts tiesās, kā arī spriedumu savstarpēja atzīšana. Ir lietderīgi no dalībvalstīm pieprasīt arī gada statistiku.

(60) Uzraudzības iestādēm būtu jānodrošina, ka vismaz reizi četros gados tiek veikta dalībvalstu sistēmu veikto datu apstrādes operāciju revīzija saskaņā ar starptautiskiem revīzijas standartiem. Revīzija būtu jāveic uzraudzības iestādēm, vai uzraudzības iestādēm būtu tieši jāpasūta revīzija no neatkarīga datu aizsardzības revidenta. Attiecīgajām uzraudzības iestādēm būtu jāsaglabā kontrole pār neatkarīgo revidentu un atbildība par viņa darbu, tāpēc tām pašām būtu jādod norādījumi revidentam un jānosaka skaidri definēts revīzijas mērķis, tvērums un metodoloģija, kā arī jānodrošina vadlīnijas un uzraudzība attiecībā uz revīziju un tās galīgajiem rezultātiem.

(61) Eiropas Datu aizsardzības uzraudzītājam būtu jāuzrauga Savienības iestāžu un struktūru darbība attiecībā uz personas datu apstrādi saskaņā ar šo regulu. Eiropas Datu aizsardzības uzraudzītājam un uzraudzības iestādēm, uzraugot *SIS*, būtu savstarpēji jāsadarbojas.

(62) Eiropas Datu aizsardzības uzraudzītājam būtu jāpiešķir pietiekami resursi saskaņā ar šo regulu uzticēto uzdevumu izpildei, tostarp atbalsts no personām, kam ir speciālās zināšanas par biometriskajiem datiem.

(63) Regulā (ES) 2016/794 ir paredzēts, ka Eiropolam jāatbalsta un jāstiprina valstu kompetento iestāžu darbības un to sadarbība terorisma un smagu noziegumu apkarošanā, un jāsniedz analīze un apdraudējumu novērtējumi. Eiropola piekļuves tiesību paplašināšanai attiecībā uz 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 minētos noziedzīgos nodarījumus, uzlabot potenciālo cietušo aizsardzību un izmeklēt nodarījumu izdarītājus. Eiropola Eiropas Kibernoziedzības centrs arī varētu gūt labumu no Eiropola, kam ir piekļuve 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.

(64) Lai novērstu trūkumus informācijas kopīgošanā par terorismu, jo īpaši par ārvalstu kaujiniekiem teroristiem – kuru pārvietošanās uzraudzība ir īpaši svarīga –, dalībvalstis tiek mudinātas kopīgot ar Eiropolu informāciju par darbībām, kas saistītas ar terorismu. Šī informācijas kopīgošana būtu jāveic kā papildinformācijas apmaiņa ar Eiropolu par attiecīgajiem brīdinājumiem. Šajā nolūkā Eiropolam būtu jāizveido savienojums ar komunikācijas infrastruktūru.

(65) Ir arī jāparedz skaidri noteikumi Eiropolam par *SIS* datu apstrādi un lejupielādi, lai tas varētu visaptveroši izmantot *SIS* ar noteikumu, ka tiek ievēroti datu aizsardzības standarti, kas paredzēti šajā regulā un Regulā (ES)2016/794. Ja Eiropola veiktā meklēšanā atklājas, ka *SIS* ir kādas dalībvalsts ievadīts brīdinājums, Eiropols nevar veikt prasīto darbību. Tādēļ tam papildinformācijas apmaiņas ceļā ar attiecīgo *SIRENE* biroju būtu jāinformē attiecīgā dalībvalsts, kas ļautu minētajai dalībvalstij izskatīt konkrēto gadījumu.

(66) Eiropas Parlamenta un Padomes Regulā (ES) 2016/1624[1] ir paredzēts, ka minētās regulas nolūkā uzņēmēja dalībvalsts atļauj minētās regulas 2. panta 8) punktā minēto vienību dalībniekiem, kurus norīko Eiropas Robežu un krasta apsardzes aģentūra, aplūkot Savienības datubāzes, ja šāda aplūkošana 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, var arī izvietot tādus ekspertus migrācijas pārvaldības atbalsta vienību sastāvā, kas nav minēto Savienības aģentūru personāls. Minētās regulas 2. panta 8) un 9) punktā minēto vienību izvietošanas mērķis ir sniegt pastiprinātu tehnisko un operatīvo palīdzību dalībvalstīm, kas izteikušas pieprasījumu, jo īpaši tām dalībvalstīm, kas saskaras ar nesamērīgām migrācijas problēmām. Lai minētās regulas 2. panta 8) un 9) punktā minētās vienības varētu pildīt tām uzticētos uzdevumus, tām ir nepieciešama piekļuve *SIS*, izmantojot Eiropas robežu un krasta apsardzes aģentūras tehnisko saskarni, kas savienota ar centrālo *SIS*. Ja meklēšanā, ko *SIS* veic Regulas (ES) 2016/1624 2. panta 8) un 9) punktā minētās vienības vai personāla vienības, tiek konstatēts dalībvalsts ievadīts brīdinājums, vienības vai personāla vienības loceklis nevar veikt prasīto darbību, izņemot, ja uzņēmēja dalībvalsts atļauj to darīt. Tādēļ uzņēmējai dalībvalstij vajadzētu būt informētai, lai tā varētu izskatīt konkrēto gadījumu. Uzņēmējai dalībvalstij būtu par informācijas atbilsmi jāpaziņo izdevējai dalībvalstij papildinformācijas apmaiņas ceļā.

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

(67) Ņemot vērā dažu *SIS* aspektu tehnisko raksturu, detalizācijas pakāpi un nepieciešamību veikt regulāru atjaunināšanu, tos nevar izsmeļoši aptvert šajā regulā. Minētie aspekti ietver, piemēram, tehniskos noteikumus par datu ievadi, par datu atjaunināšanu, dzēšanu un meklēšanu un par datu kvalitāti, un noteikumus, kas saistīti ar biometriskajiem datiem, noteikumus attiecībā uz brīdinājumu savietojamību un prioritāro secību, par brīdinājumu sasaisti, brīdinājumu beigu termiņu noteikšanu maksimālo termiņu ietvaros un par papildinformācijas apmaiņu. Īstenošanas pilnvaras attiecībā uz minētajiem aspektiem tāpēc būtu jāpiešķir Komisijai. Tehniskajos noteikumos brīdinājumu meklēšanai būtu jāņem vērā valstu sistēmu raita darbība.

(68) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, Komisijai būtu jāpiešķir īstenošanas pilnvaras. Minētās pilnvaras būtu jāīsteno saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011[1]. Īstenošanas aktu pieņemšanas procedūrai vajadzētu būt tādai pašai gan šajā regulā, gan Regulā (ES) 2018/...[+].

(69) Pārredzamības nodrošināšanai divus gadus pēc *SIS* darbības sākuma, ievērojot šo regulu, *eu-LISA* būtu jāizstrādā ziņojums par centrālās *SIS* un komunikācijas infrastruktūras tehnisko darbību, tostarp to drošību, un par papildinformācijas divpusēju un daudzpusēju apmaiņu. Komisijai ik pēc četriem gadiem būtu jāveic vispārējs novērtējums.

---

[1] 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.).

[+] OV: lūgums tekstā ievietot numuru dokumentā PE-CONS 35/18 iekļautajai regulai.

(70) Lai nodrošinātu *SIS* raitu darbību, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu attiecībā uz jaunām priekšmetu apakškategorijām, kas jāmeklē saistībā ar brīdinājumiem par priekšmetiem izņemšanai vai kas izmantotas par pierādījumu kriminālprocesā, un to apstākļu noteikšanu, kad būtu jāatļauj sejas attēlu un fotogrāfiju izmantošana personu identifikācijai, kas nav saistībā ar regulārajām robežšķērsošanas vietām. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu[1]. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.

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

[1] OV L 123, 12.5.2016., 1. lpp.

(72) Šajā regulā tiek ievērotas pamattiesības un principi, kas jo īpaši atzīti Eiropas Savienības Pamattiesību hartā. Jo īpaši šajā regulā tiek pilnībā ievērota personas datu aizsardzība saskaņā ar Eiropas Savienības Pamattiesību hartas 8. pantu, vienlaikus tiecoties nodrošināt drošu vidi visām personām, kas dzīvo Savienības teritorijā, un īpašu aizsardzību bērniem, kuri varētu kļūt par cietušajiem cilvēku tirdzniecībā vai nolaupīšanā. Lietās, kas attiecas uz bērniem, pirmām kārtām būtu jāņem vērā bērna intereses.

(73) Saskaņā ar 1. un 2. pantu Protokolā Nr. 22 par Dānijas nostāju, kas pievienots LES un LESD, 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.

(74) Apvienotā Karaliste piedalās šajā regulā saskaņā ar 5. panta 1. punktu Protokolā Nr. 19 par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā, kas pievienots LES un LESD, un 8. panta 2. punktu Padomes Lēmumā 2000/365/EK[1].

[1] Padomes Lēmums 2000/365/EK (2000. gada 29. maijs) par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā (OV L 131, 1.6.2000., 43. lpp.).

(75) Īrija piedalās šajā regulā saskaņā ar 5. panta 1. punktu Protokolā Nr. 19, kas pievienots LES un LESD, un 6. panta 2. punktu Padomes Lēmumā 2002/192/EK[1].

(76) 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[2], šī regula ir to Šengenas *acquis* noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta 1. panta G. punktā Padomes Lēmumā 1999/437/EK[3].

---

1 Padomes Lēmums 2002/192/EK (2002. gada 28. februāris) par Īrijas lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā (OV L 64, 7.3.2002., 20. lpp.).

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

3 Padomes Lēmums 1999/437/EK (1999. gada 17. maijs) par dažiem pasākumiem, lai piemērotu Eiropas Savienības Padomes, Islandes Republikas un Norvēģijas Karalistes Nolīgumu par abu minēto valstu iesaistīšanos Šengenas *acquis* īstenošanā, piemērošanā un izstrādē (OV L 176, 10.7.1999., 31. lpp.).

(77) Attiecībā uz Šveici – saskaņā ar Nolīgumu starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā[1] 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 2008/149/TI[2] 3. pantu.

---

[1] OV L 53, 27.2.2008., 52. lpp.

[2] Padomes Lēmums 2008/149/TI (2008. gada 28. janvāris) par to, lai Eiropas Savienības vārdā noslēgtu Nolīgumu starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā (OV L 53, 27.2.2008., 50. lpp.).

(78) 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[1] 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[2] 3. pantu.

---

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

2 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.).

(79) Attiecībā uz Bulgāriju un Rumāniju šī regula ir akts, kas pilnveido Šengenas *acquis* vai ir kā citādi saistīts ar to, kā noteikts 2005. gada Pievienošanās akta 4. panta 2. punktā, un būtu jālasa saistībā ar Padomes Lēmumiem 2010/365/ES[1] un (ES) 2018/934[2].

(80) Attiecībā uz Horvātiju šī regula ir akts, kas pilnveido Šengenas *acquis* vai ir kā citādi saistīts ar to, kā noteikts 2011. gada Pievienošanās akta 4. panta 2. punktā, un būtu jālasa saistībā ar Padomes Lēmumu 2017/733[3].

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

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

---

1 Padomes Lēmums 2010/365/ES (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.).

2 Padomes Lēmums (ES) 2018/934 (2018. gada 25. jūnijs) par atlikušo Šengenas *acquis* noteikumu īstenošanu saistībā ar Šengenas Informācijas sistēmu Bulgārijas Republikā un Rumānijā (OV L 165, 2.7.2018., 37. lpp.).

3 Padomes Lēmums (ES) 2017/733 (2017. gada 25. aprīlis) par Šengenas *acquis* noteikumu piemērošanu attiecībā uz Šengenas Informācijas sistēmu Horvātijas Republikā (OV L 108, 26.4.2017., 31. lpp.).

(83) Ar šo regulu tiek ieviesti vairāki uzlabojumi *SIS*, kas palielinās tās efektivitāti, stiprinās datu aizsardzību un paplašinās piekļuves tiesības. Dažiem no minētajiem uzlabojumiem nav vajadzīga sarežģīta tehniska izstrāde, turpretī citiem ir nepieciešamas dažāda līmeņa tehniskas izmaiņas. Lai sistēmas uzlabojumi būtu pieejami galalietotājiem pēc iespējas ātrāk, ar šo regulu ievieš grozījumus Lēmumā 2007/533/TI vairākos posmos. Vairāki sistēmas uzlabojumi būtu jāpiemēro nekavējoties pēc šīs regulas stāšanās spēkā, savukārt citi būtu jāpiemēro vai nu gadu vai divus pēc tās stāšanās spēkā. Šī regula pilnībā būtu jāpiemēro trīs gadu laikā pēc tās stāšanās spēkā. Lai novērstu kavēšanos šīs regulas piemērošanā, tās pakāpeniskā īstenošana būtu cieši jāuzrauga.

(84) Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1986/2006[1], Lēmumu 2007/533/TI un Komisijas Lēmumu 2010/261/ES[2] būtu jāatceļ no dienas, kad pilnībā sāk piemērot šo regulu.

(85) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001[3] 28. panta 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas atzinumu sniedza 2017. gada 3. maijā,

IR PIEŅĒMUŠI ŠO REGULU.

---

1 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.).

2 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.).

3 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.).

I NODAĻA
VISPĀRĪGI NOTEIKUMI

1. pants

SIS *vispārējais mērķis*

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

2. pants

Priekšmets

1. Ar šo regulu paredz nosacījumus un kārtību tādu brīdinājumu ievadīšanai un apstrādei *SIS*, kas izdoti attiecībā uz personām un priekšmetiem, un par papildinformācijas un papildu datu apmaiņu ar mērķi policijas un tiesu iestādēm sadarboties krimināllietās.

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

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "brīdinājums" ir datu kopums, ko ievada *SIS* un kas kompetentajām iestādēm ļauj identificēt personu vai priekšmetu, lai konkrēti rīkotos;

2) "papildinformācija" ir informācija, kas nav *SIS* saglabāto brīdinājuma datu sastāvdaļa, bet ir saistīta ar brīdinājumiem *SIS* un kuras apmaiņa jāveic ar *SIRENE* biroju starpniecību:

   a) lai dalībvalstis varētu apspriesties vai informēt cita citu, ievadot brīdinājumu,

   b) pēc tam, kad ir konstatēta informācijas atbilsme, lai varētu attiecīgi rīkoties,

   c) ja nav iespējams veikt prasīto darbību,

   d) attiecībā uz *SIS* datu kvalitāti,

   e) attiecībā uz brīdinājumu savietojamību un prioritāti,

   f) attiecībā uz piekļuves tiesībām;

3) "papildu dati" ir dati, ko saglabā *SIS* un kas ir saistīti ar brīdinājumiem *SIS* un nekavējoties pieejami kompetentajām iestādēm, ja, veicot meklēšanu *SIS*, tiek atrasta persona, par kuru dati ir ievadīti *SIS*;

4) "personas dati" ir personas dati, kā definēts Regulas (ES) 2016/679 4. panta 1) punktā;

5) "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, ierakstīšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, izgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

6) "atbilstība" ir šādu posmu norise:

a) meklēšanu *SIS* ir veicis galalietotājs,

b) minētajā meklēšanā tiek konstatēts brīdinājums, ko *SIS* ir ievadījusi cita dalībvalsts, un

c) dati, kas attiecas uz brīdinājumu *SIS*, atbilst meklētajiem datiem;

7) "informācijas atbilsme" ir jebkura atbilstība, kas atbilst šādiem kritērijiem:

a) to ir apstiprinājis:

i) galalietotājs, vai

ii) kompetentā iestāde saskaņā ar valsts procedūrām, ja attiecīgā atbilstība bija balstīta uz biometrisko datu salīdzināšanu,

un

b) tiek pieprasīts veikt turpmākas darbības;

8) "atzīme" ir brīdinājuma derīguma apturēšana valsts līmenī, ko var pievienot brīdinājumiem par apcietināšanu, brīdinājumiem par pazudušām un neaizsargātām personām un brīdinājumiem par diskrētu, izmeklēšanas un īpašu pārbaudi;

9) "izdevēja dalībvalsts" ir dalībvalsts, kas ir ievadījusi brīdinājumu *SIS*;

10) "izpildītāja dalībvalsts" ir dalībvalsts, kas pēc tam, kad ir konstatēta informācijas atbilsme, veic vai ir veikusi prasītās darbības;

11) "galalietotājs" ir kompetentās iestādes darbinieks, kas pilnvarots tieši meklēt *CS-SIS*, *N.SIS* vai to tehniskajā kopijā;

12) "biometriskie dati" ir tādi personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām vai psiholoģiskajām pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, proti, fotogrāfijas, sejas attēli, daktiloskopiskie dati un DNS profili;

13) "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;

14) "sejas attēls" ir sejas digitālie attēli ar pietiekamu attēla izšķirtspēju un kvalitāti, lai tos varētu izmantot automatizētai biometrisko datu salīdzināšanai;

15) "DNS profils" ir burtu vai ciparu kods, kurā ir atveidots analizētā cilvēka DNS parauga nekodētās daļas identifikācijas parametru komplekss, proti, konkrēta dažādu DNS vietu (loci) molekulu struktūra;

16) "teroristu nodarījumi" ir valsts tiesību aktos noteiktie nodarījumi, kas minēti Eiropas Parlamenta un Padomes Direktīvas (ES) 2017/541[1] 3. līdz 14. pantā, vai – attiecībā uz dalībvalstīm, kurām minētā direktīva nav saistoša, – ir līdzvērtīgi vienam no minētajiem nodarījumiem;

17) "sabiedrības veselības apdraudējums" ir sabiedrības veselības apdraudējums, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2016/399[2] 2. panta 21. punktā.

4. pants

SIS *tehniskā uzbūve un darbības veidi*

1. *SIS* veido:

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

i) tehniskā nodrošinājuma vienība ("*CS-SIS*"), kurā ietverta datubāze ("*SIS* datubāze"), tostarp rezerves *CS-SIS*,

ii) vienota valsts saskarne ("*NI-SIS*");

b) valsts sistēma (*N.SIS*) katrā dalībvalstī, ko veido valsts datu sistēmas, kuras ir saistītas ar centrālo *SIS*, tostarp vismaz viena valsts vai kopīgota rezerves *N.SIS*; un

---

[1] Eiropas Parlamenta un Padomes Direktīva (ES) 2017/541 (2017. gada 15. marts) par terorisma apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2002/475/TI un groza Padomes Lēmumu 2005/671/TI (OV L 88, 31.3.2017., 6. lpp.).

[2] Eiropas Parlamenta un Padomes Regula (ES) 2016/399 (2016. gada 9. marts) par Savienības Kodeksu par noteikumiem, kas reglamentē personu pārvietošanos pār robežām (Šengenas Robežu kodekss) (OV L 77, 23.3.2016., 1. lpp.).

c) *CS-SIS*, rezerves *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.

N.SIS, kā minēts b) apakšpunktā, var ietvert datu datni ("valsts kopija"), kas ir pilnīga vai daļēja *SIS* datubāzes kopija. Divas vai vairāk dalībvalstis var vienā no savām *N.SIS* izveidot kopīgotu kopiju, kuru minētās dalībvalstis var izmantot kopīgi. Šādu kopīgotu kopiju uzskata par katras minētās dalībvalsts valsts kopiju.

Kopīgotu rezerves *N.SIS*, kā minēts b) apakšpunktā, var kopīgi izmantot divas vai vairāk dalībvalstis. Šādos gadījumos kopīgoto rezerves *N.SIS* uzskata par katras minētās dalībvalsts rezerves *N.SIS*. *N.SIS* un rezerves *N.SIS* var izmantot vienlaicīgi, lai nodrošinātu nepārtrauktu pieejamību galalietotājiem.

Dalībvalstis, kas plāno izveidot kopīgotu kopiju vai kopīgotu rezerves *N.SIS*, kuru kopīgi lietot, rakstiski vienojas par saviem attiecīgajiem pienākumiem. Tās par viņu vienošanos paziņo Komisijai.

Komunikācijas infrastruktūra atbalsta un sekmē *SIS* nepārtrauktas pieejamības nodrošināšanu. Tā ietver rezerves un nodalītus ceļus savienojumiem starp *CS-SIS* un rezerves *CS-SIS*, un tajā ir ietverti arī rezerves un nodalīti ceļi savienojumiem starp katru *SIS* tīkla valsts piekļuves punktu un *CS-SIS* un rezerves *CS-SIS*.

2. Dalībvalstis ievada, atjaunina, dzēš *SIS* datus un veic tajos meklēšanu, izmantojot katra savu *N.SIS*. Dalībvalstis, kas lieto daļēju vai pilnīgu valsts kopiju vai daļēju vai pilnīgu kopīgotu kopiju, dara minēto kopiju pieejamu, lai veiktu automatizētu meklēšanu katras minētās dalībvalsts teritorijā. Daļējā valsts vai kopīgotā kopija ietver vismaz tos datus, kas uzskaitīti šīs regulas 20. panta 3. punkta a) – v) apakšpunktā. Veikt meklēšanu citu dalībvalstu *N.SIS* datu datnēs nav iespējams, izņemot kopīgotu kopiju gadījumā.

3. *CS-SIS* veic tehniskās uzraudzības un administrācijas uzdevumus, un tai ir rezerves *CS-SIS*, kas spēj nodrošināt visas galvenās *CS-SIS* funkcijas minētās sistēmas avārijas gadījumā. *CS-SIS* un rezerves *CS-SIS* atrodas divos tehniskajos *eu-LISA* centros.

4. *eu-LISA* īsteno tehniskus risinājumus ar mērķi pastiprināt *SIS* nepārtrauktu pieejamību, vai nu nodrošinot *CS-SIS* un rezerves *CS-SIS* vienlaicīgu darbību – ar noteikumu, ka rezerves *CS-SIS* spēj nodrošināt *SIS* darbību *CS-SIS* avārijas gadījumā –, vai arī dublējot sistēmu vai tās komponentus. Neatkarīgi no procedūras prasībām, kas noteiktas Regulas (ES) 2018/...[+] 10. pantā, *eu-LISA* ne vēlāk kā … [viens gads pēc šīs regulas stāšanās spēkā] sagatavo pētījumu par tehnisko risinājumu iespējām, kurā ir iekļauts neatkarīgs ietekmes novērtējums un izmaksu un ieguvumu analīze.

5. Vajadzības gadījumā izņēmuma apstākļos *eu-LISA* var uz laiku izstrādāt *SIS* datubāzes papildu kopiju.

[+] OV: lūgums ievietot dokumentā PE-CONS 29/18 ietvertās regulas numuru.

6. *CS-SIS* nodrošina pakalpojumus, kas vajadzīgi, lai ievadītu un apstrādātu *SIS* datus, tostarp veiktu meklēšanu *SIS* datubāzē. Dalībvalstīm, kas lieto valsts vai kopīgotu kopiju, *CS-SIS* nodrošina:

   a) valsts kopiju tiešsaistes atjaunināšanu;

   b) valsts kopiju un *SIS* datu bāzes sinhronizāciju un saskanību; un

   c) kārtību valsts kopiju inicializēšanai un rekonstrukcijai;

7. *CS-SIS* nodrošina nepārtrauktu pieejamību.

5. pants

Izmaksas

1. Centrālās *SIS* un komunikācijas infrastruktūras darbības, uzturēšanas un turpmākas izstrādes izmaksas sedz no Savienības vispārējā budžeta. Minētās izmaksas ietver attiecībā uz *CS-SIS* veikto darbu, lai nodrošinātu 4. panta 6. punktā minēto pakalpojumu sniegšanu.

2. 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 tās sasaistīšanu ar *NI-SIS*.

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

Katra dalībvalsts nosūta brīdinājumus ar savas *N.SIS* starpniecību.

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* raitu 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.

2. Katra dalībvalsts norīko valsts iestādi, kas darbojas 24 stundas diennaktī septiņas dienas nedēļā un kas nodrošina visas papildinformācijas apmaiņu un pieejamību (*SIRENE* birojs) saskaņā ar *SIRENE* rokasgrāmatas noteikumiem. Katrs *SIRENE* birojs ir vienots kontaktpunkts savai dalībvalstij nolūkā apmainīties ar papildinformāciju par brīdinājumiem un atvieglot prasīto darbību veikšanu gadījumos, kad brīdinājumi par personām vai priekšmetiem ir ievadīti *SIS* un minētās personas vai priekšmeti tiek atrasti informācijas atbilsmes rezultātā.

Katram *SIRENE* birojam saskaņā ar valsts tiesību aktiem ir ērta tieša vai netieša piekļuve visai attiecīgajai valsts informācijai, tostarp valsts datubāzēm un visai informācijai par savas dalībvalsts brīdinājumiem, kā arī ekspertu padomiem, lai varētu ātri un 8. pantā paredzētajos termiņos reaģēt uz lūgumiem sniegt papildinformāciju.

SIRENE biroji koordinē *SIS* ievadītās informācijas kvalitātes pārbaudi. Minētajos nolūkos tiem ir piekļuve *SIS* apstrādātajiem datiem.

3. Dalībvalstis sniedz *eu-LISA* ziņas par savu valsts *N.SIS* biroju un *SIRENE* biroju. *eu-LISA* publicē *N.SIS* biroju un *SIRENE* biroju sarakstu kopā ar 56. panta 7. punktā minēto sarakstu.

8. pants

Papildinformācijas apmaiņa

1. Papildinformācijas apmaiņu veic saskaņā ar *SIRENE* rokasgrāmatas noteikumiem un izmantojot komunikācijas infrastruktūru. Dalībvalstis nodrošina nepieciešamos tehniskos resursus un cilvēkresursus, lai nodrošinātu papildinformācijas nepārtrauktu pieejamību un savlaicīgu un efektīvu apmaiņu ar to. Gadījumā, ja komunikācijas infrastruktūra nav pieejama, dalībvalstis papildinformācijas apmaiņai izmanto citus atbilstīgi nodrošinātus tehniskos līdzekļus. Atbilstīgi nodrošinātu tehnisko līdzekļu sarakstu paredz *SIRENE* rokasgrāmatā.

2. Papildinformāciju izmanto vienīgi nolūkā, kādā tā ir nosūtīta saskaņā ar 64. pantu, izņemot, ja no izdevējas dalībvalsts ir saņemta iepriekšēja piekrišana citādai izmantošanai.

3. *SIRENE* biroji veic savus uzdevumus ātri un efektīvi, jo īpaši, atbildot uz lūgumu sniegt papildinformāciju pēc iespējas drīz, bet ne vēlāk kā 12 stundu laikā pēc lūguma saņemšanas. *SIRENE* biroji rīkojas nekavējoties, ja ir brīdinājumi par teroristu nodarījumiem, brīdinājumi par personām, kuras meklē, lai apcietinātu nolūkā tās nodot vai izdot, un brīdinājumi par bērniem, kā minēts 32. panta 1. punkta c) apakšpunktā.

   Lūgumus sniegt papildinformāciju ar visaugstāko prioritāti *SIRENE* veidlapās apzīmē ar norādi "*URGENT*", kā arī norāda steidzamības iemeslu.

4. Komisija pieņem īstenošanas aktus, lai paredzētu sīki izstrādātus noteikumus par *SIRENE* biroju uzdevumiem, ievērojot šo regulu, un par papildinformācijas apmaiņu kā rokasgrāmatu, kas tiek saukta par "*SIRENE* rokasgrāmatu". Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

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 centrālo *SIS*.

2. Ja dalībvalsts izmanto valsts kopiju, tā ar *CS-SIS* sniegtu pakalpojumu un 4. panta 6. punktā minēto automātisko atjaunināšanu palīdzību nodrošina, ka dati, ko glabā valsts kopijā, ir identiski un saskaņoti ar *SIS* datubāzi un ka meklēšana tās valsts kopijā sniedz līdzvērtīgu rezultātu *SIS* datubāzē veiktai meklēšanai.

3. Galalietotāji saņem datus, kas ir vajadzīgi, lai veiktu savus uzdevumus, jo īpaši un vajadzības gadījumā visus pieejamos datus, kas nodrošina datu subjekta identifikāciju un iespēju veikt prasīto darbību.

4. Dalībvalstis un *eu-LISA* regulāri veic testus, lai pārbaudītu 2. punktā minēto valsts kopiju tehnisko atbilstību. Minēto testu rezultātus ņem vērā kā daļu no mehānisma, kas izveidots ar Padomes Regulu (ES) Nr. 1053/2013[1].

5. Komisija pieņem īstenošanas aktus, lai noteiktu un pilnveidotu šā panta 1. punktā minētos kopīgos standartus, protokolus un tehniskās procedūras. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

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);

[1] 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.).

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) novērstu datu neatļautu apstrādi *SIS*, kā arī *SIS* apstrādātu datu jebkādu neatļautu grozīšanu vai dzēšanu (datu ievades kontrole);

g) nodrošinātu, ka personām, kas ir pilnvarotas izmantot datu apstrādes automatizētu sistēmu, ir piekļuve tikai tiem datiem, uz kuriem attiecas viņu piekļuves pilnvarojums, piekļuvei izmantojot individuālus un unikālus lietotāja identifikatorus un konfidenciālus piekļuves režīmus (datu piekļuves kontrole);

h) 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 69. panta 1. punktā minēto uzraudzības iestāžu lūguma minētos profilus bez kavēšanās dara tām pieejamus (personālie profili);

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

j) 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);

k) 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);

l) uzraudzītu šajā punktā minēto aizsardzības pasākumu efektivitāti un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību, lai nodrošinātu atbilstību šai regulai (paškontrole);

m) nodrošinātu, ka darbības traucējumu gadījumā uzstādīto sistēmu darbību var atjaunot parastā režīmā (darbības atjaunošana); un

n) nodrošinātu, ka *SIS* savas funkcijas pilda pareizi, par kļūdu parādīšanos darbībās tiek ziņots (uzticamība) un *SIS* saglabātie personas dati nevar tikt sabojāti sistēmas darbības traucējumu dēļ (integritāte).

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

3. Dalībvalstis pieņem šā panta 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar *SIS* datu apstrādi, ko veic iestādes, kas minētas 44. pantā.

4. Šā panta 1., 2. un 3. punktā aprakstītie pasākumi var būt daļa no vispārīgas pieejas drošībai un plāna valsts līmenī, aptverot vairākas IT sistēmas. Šādos gadījumos minētajā plānā ir skaidri identificējamas šajā pantā izklāstītās prasības un to piemērojamība *SIS*, un tās tiek ar minēto plānu nodrošinātas.

11. pants

Konfidencialitāte – dalībvalstis

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

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

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

12. pants

Reģistra ierakstu glabāšana valstīs

1. Dalībvalstis nodrošina, ka katra piekļuve personas datiem un visas personas datu apmaiņas *CS-SIS* ietvaros tiek ierakstītas reģistrā *N.SIS*, lai varētu pārbaudīt, vai meklēšana bija likumīga, lai uzraudzītu datu apstrādes likumību, pašuzraudzības nolūkos, lai nodrošinātu *N.SIS* pareizu darbību, kā arī datu integritāti un drošību. Šī prasība neattiecas uz 4. panta 6. punkta a), b) un c) apakšpunktā minētajiem automātiskajiem procesiem.

2. Reģistra ieraksti konkrēti parāda brīdinājuma vēsturi, datu apstrādes darbības datumu un laiku, meklēšanā izmantoto datu veidu, atsauci uz apstrādāto datu veidu un gan kompetentās iestādes, gan datus apstrādājošās personas individuālus un unikālus lietotāja identifikatorus.

3. Atkāpjoties no šā panta 2. punkta, ja meklēšana tiek veikta ar daktiloskopiskajiem datiem vai sejas attēlu saskaņā ar 43. pantu, reģistra ieraksti parāda meklēšanā izmantoto datu veidu, nevis faktiskos datus.

4. Reģistra ierakstus lieto vienīgi 1. punktā minētajā nolūkā, un tos dzēš pēc trim gadiem no to izveides dienas. Reģistra ierakstus, kuros ietverta brīdinājumu vēsture, dzēš trīs gadus pēc brīdinājumu dzēšanas.

5. Reģistra ierakstus var saglabāt ilgāk par 4. punktā minēto laikposmu, ja tie vajadzīgi uzraudzības procedūrām, kas jau ir iesāktas.

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

7. Ja dalībvalstis saskaņā ar valsts tiesību aktiem veic transportlīdzekļu numuru zīmju automatizētu skenēšanas meklēšanu, izmantojot automatizētas numura zīmes atpazīšanas sistēmas, dalībvalstis glabā ierakstus par meklēšanu saskaņā ar valsts tiesību aktiem. Vajadzības gadījumā var veikt pilnu meklēšanu *SIS*, lai pārbaudītu, vai ir konstatēta informācijas atbilsme. Jebkādai pilnai meklēšanai piemēro 1. līdz 6. punktu.

8. Komisija pieņem īstenošanas aktus, lai noteiktu šā panta 7. punktā minētā reģistra ieraksta saturu. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

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 uzraudzības iestādi.

14. pants

Personāla apmācība

1. 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, par pamattiesībām, tostarp datu aizsardzību, un par datu apstrādes noteikumiem un procedūrām, kuras izklāstītas *SIRENE* rokasgrāmatā. Darbiniekus informē par visiem attiecīgajiem noteikumiem par noziedzīgajiem nodarījumiem un sankcijām, tostarp tām, kas paredzētas šīs regulas 73. pantā.

2. Dalībvalstīs darbojas valsts līmeņa *SIS* apmācības programma, kurā notiek gan galalietotāju, gan arī *SIRENE* biroju darbinieku apmācība.

   Minētā apmācības programma var būt daļa no vispārīgas apmācības programmas valsts līmenī, kas aptver apmācību citās svarīgās jomās.

3. Savienības līmenī vismaz reizi gadā organizē kopīgus apmācības kursus, lai uzlabotu sadarbību starp *SIRENE* birojiem.

III NODAĻA
eu-LISA ATBILDĪBA

15. pants

Darbības pārvaldība

1. Par centrālās *SIS* darbības pārvaldību atbild *eu-LISA*. Sadarbībā ar dalībvalstīm *eu-LISA* nodrošina to, ka centrālās *SIS* vajadzībām vienmēr tiek izmantota vislabākā pieejamā tehnoloģija, pamatojoties uz izmaksu un ieguvumu analīzi.

2. *eu-LISA* ir atbildīga arī par šādiem uzdevumiem, kas saistīti ar komunikācijas infrastruktūru:

   a) uzraudzība;

   b) drošība;

   c) dalībvalstu un nodrošinātāja attiecību koordinēšana;

   d) uzdevumiem saistībā ar budžeta izpildi;

   e) iegādi un atjaunināšanu; un

   f) jautājumiem, kas saistīti ar līgumiem.

3. *eu-LISA* ir atbildīga arī par šādiem uzdevumiem, kas saistīti ar *SIRENE* birojiem un komunikāciju starp *SIRENE* birojiem:

a) koordinēt, vadīt un atbalstīt testēšanas pasākumus;

b) uzturēt un atjaunināt tehniskās specifikācijas papildinformācijas apmaiņai starp *SIRENE* birojiem un komunikācijas infrastruktūru; un

c) pārvaldīt tehnisko izmaiņu ietekmi, ja tā skar gan *SIS*, gan papildinformācijas apmaiņu starp *SIRENE* birojiem.

4. *eu-LISA* izstrādā un uztur mehānismu un procedūras, lai veiktu *CS-SIS* datu kvalitātes pārbaudes. Šajā sakarā tā regulāri iesniedz ziņojumus dalībvalstīm.

eu-LISA regulāri iesniedz Komisijai ziņojumu par problēmām, kas radušās, un attiecīgajām dalībvalstīm.

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

5. *eu-LISA* veic arī uzdevumus, kas saistīti ar apmācības nodrošināšanu par *SIS* tehnisko izmantošanu un par pasākumiem *SIS* datu kvalitātes uzlabošanai.

6. Centrālās *SIS* darbības pārvaldība ir visi uzdevumi, kas vajadzīgi, lai saskaņā ar šo regulu nodrošinātu centrālās *SIS* darbību 24 stundas diennaktī 7 dienas nedēļā, jo īpaši uzturēšanas darbi un tehniski pielāgojumi, kas vajadzīgi sistēmas raitai darbībai. Minētie uzdevumi ietver arī centrālās *SIS* un *N.SIS* testēšanas pasākumu koordinēšanu, vadību un atbalstīšanu, kas nodrošina, ka centrālā *SIS* un *N.SIS* darbojas saskaņā ar tehniskās un funkcionālās atbilstības prasībām, kas izklāstītas 9. pantā.

7. Komisija pieņem īstenošanas aktus, lai noteiktu komunikācijas infrastruktūras tehniskās prasības. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 76. panta 2. punktā.

16. pants

Drošība – eu-LISA

1. Attiecībā uz centrālo *SIS* un komunikācijas infrastruktūru *eu-LISA* 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) novērstu datu neatļautu apstrādi *SIS*, kā arī *SIS* apstrādātu datu jebkādu neatļautu grozīšanu vai dzēšanu (datu ievades kontrole);

g) nodrošinātu, ka personām, kas ir pilnvarotas izmantot datu apstrādes automatizētu sistēmu, ir piekļuve tikai tiem datiem, uz kuriem attiecas viņu piekļuves pilnvarojums, piekļuvei izmantojot individuālus un unikālus lietotāja identifikatorus un konfidenciālus piekļuves režīmus (datu piekļuves kontrole);

h) izstrādātu profilus, raksturojot to personu funkcijas un pienākumus, kuras ir pilnvarotas piekļūt datiem vai datu apstrādes iekārtām, un pēc Eiropas Datu aizsardzības uzraudzītāja lūguma minētos profilus nekavējoties darītu tam pieejamus (personālie profili);

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

j) 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);

k) nodrošinātu to, ka personas datu nosūtīšanas un datu nesēju pārsūtīšanas laikā nav iespējama datu neatļauta lasīšana, kopēšana, grozīšana vai dzēšana, jo īpaši ar attiecīgiem kodēšanas paņēmieniem (pārsūtīšanas kontrole);

l) uzraudzītu šajā punktā minēto aizsardzības pasākumu efektivitāti un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību, lai nodrošinātu atbilstību šai regulai (paškontrole);

m) nodrošinātu, ka darbības traucējumu gadījumā uzstādīto sistēmu darbību var atjaunot parastā režīmā (darbības atjaunošana);

n) nodrošinātu, ka *SIS* savas funkcijas pilda pareizi, par kļūdu parādīšanos darbībās tiek ziņots (uzticamība) un *SIS* saglabātie personas dati nevar tikt sabojāti sistēmas darbības traucējumu dēļ (integritāte); un

o) nodrošinātu tās tehnisko centru drošību.

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

17. pants

Konfidencialitāte – eu-LISA

1. Neskarot Civildienesta noteikumu 17. pantu, *eu-LISA* 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. Minētais pienākums ir spēkā arī pēc tam, kad minētās personas vairs neieņem attiecīgo amatu vai netiek nodarbinātas, vai viņu darbība ir izbeigta.

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

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

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

18. pants

Reģistra ierakstu glabāšana centrālajā līmenī

1. *eu-LISA* nodrošina, ka 12. panta 1. punktā noteiktajiem mērķiem tiek saglabāti reģistra ieraksti par katru piekļuvi *CS-SIS* saglabātajiem personas datiem un par visām minēto datu apmaiņām.

2. Reģistra ieraksti konkrēti parāda brīdinājuma vēsturi, datu apstrādes darbības datumu un laiku, meklēšanā izmantoto datu veidu, atsauci uz apstrādāto datu veidu un kompetentās iestādes, kas apstrādā datus, individuālus un unikālus lietotāja identifikatorus.

3. Atkāpjoties no šā panta 2. punkta, ja meklēšana tiek veikta ar daktiloskopiskajiem datiem vai sejas attēliem saskaņā ar 43. pantu, reģistra ieraksti parāda meklēšanā izmantoto datu veidu, nevis faktiskos datus.

4. Reģistra ierakstus lieto vienīgi 1. punktā minētajos nolūkos, un tos dzēš pēc trim gadiem no to izveides dienas. Reģistra ierakstus, kuros ietverta brīdinājumu vēsture, dzēš trīs gadus pēc brīdinājumu dzēšanas.

5. Reģistra ierakstus var glabāt ilgāk par 4. apakšpunktā minētajiem laikposmiem, ja tie vajadzīgi uzraudzības procedūrām, kas jau ir iesāktas.

6. Lai veiktu pašuzraudzību un nodrošinātu *CS-SIS* pareizu darbību, datu integritāti un drošību, *eu-LISA* atbilstīgi tās kompetencei ir piekļuve reģistra ierakstiem.

Eiropas Datu aizsardzības uzraudzītājam pēc lūguma un atbilstīgi tā kompetencei ir piekļuve minētajiem reģistra ierakstiem, lai tas varētu pildīt savus pienākumus.

IV NODAĻA
SABIEDRĪBAS INFORMĒŠANA

19. pants

SIS informācijas kampaņas

Šīs regulas piemērošanas sākumposmā Komisija sadarbībā ar uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju īsteno kampaņu, lai informētu sabiedrību par *SIS* mērķiem, *SIS* glabātajiem datiem, iestādēm, kurām ir piekļuve *SIS*, un datu subjektu tiesībām. Komisija regulāri atkārto šādas kampaņas sadarbībā ar uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju. Komisija uztur publiski pieejamu tīmekļa vietni, kurā sniegta visa attiecīgā informācija, kas saistīta ar *SIS*. Dalībvalstis sadarbībā ar savām uzraudzības iestādēm izstrādā un īsteno vajadzīgās rīcībpolitikas, lai informētu savus pilsoņus un iedzīvotājus par *SIS* kopumā.

V NODAĻA
DATU KATEGORIJAS UN BRĪDINĀJUMU APZĪMĒŠANA AR ATZĪMĒM

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., 38. un 40. pantā noteiktajiem nolūkiem.

2. Datu kategorijas ir šādas:

   a) informācija par personām, attiecībā uz kurām ievadīts brīdinājums;

   b) informācija par priekšmetiem, kas minēti 26., 32., 34., 36. un 38. pantā.

3. Jebkurš brīdinājums *SIS*, kurā ir ietverta informācija par personām, ietver tikai šādus datus:

   a) uzvārdi;

   b) vārdi;

   c) 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) visas valstspiederības;

j) norāde, vai attiecīgā persona:

i) ir bruņota;

ii) ir vardarbīga;

iii) ir aizbēgusi vai izbēgusi;

iv) ir pakļauta pašnāvības riskam;

v) rada sabiedrības veselības apdraudējumu; vai

vi) ir iesaistīta kādā Direktīvas (ES) 2017/541 3.–14. pantā minētā darbībā;

k) brīdinājuma iemesls;

l) iestāde, kas izveidojusi brīdinājumu;

m) norāde uz lēmumu, kas ir brīdinājuma pamatā;

n) informācijas atbilsmes gadījumā veicamā darbība;

o) sasaiste ar citiem brīdinājumiem, ievērojot 63. pantu;

p) noziedzīgā nodarījuma veids;

q) personas reģistrācijas numurs valsts reģistrā;

r) attiecībā uz brīdinājumiem, kas minēti 32. panta 1. punktā, – gadījuma veids atbilstoši kategorijai;

s) personas identifikācijas dokumentu kategorija;

t) personas identifikācijas dokumentu izdošanas valsts;

u) personas identifikācijas dokumentu numurs(-i);

v) personas identifikācijas dokumentu izdošanas datums;

w) fotogrāfijas un sejas attēli;

x) saskaņā ar 42. panta 3. punktu – attiecīgie DNS profili;

y) daktiloskopiskie dati;

z) identifikācijas dokumentu kopija, ja iespējams – krāsu.

4. Komisija pieņem īstenošanas aktus, lai noteiktu un pilnveidotu tehniskos noteikumus, kas nepieciešami, lai ievadītu, atjauninātu, dzēstu un meklētu datus, kas minēti šā panta 2. un 3. punktā, un vienotos standartus, kas minēti šā panta 5. punktā. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

5. Tehniskie noteikumi ir līdzīgi tehniskajiem noteikumiem attiecībā uz meklēšanu *CS-SIS*, valsts vai kopīgotajās kopijās un tehniskajās kopijās, kas izveidotas saskaņā ar 56. panta 2. punktu. Tie ir balstīti uz vienotiem standartiem.

21. pants

Samērīgums

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

2. Ja personu vai priekšmetu meklē saistībā ar brīdinājumu par teroristu nodarījumu, konkrēto gadījumu uzskata par atbilstīgu, piemērotu un pietiekami svarīgu, lai būtu brīdinājums *SIS*. Sabiedriskās vai valsts drošības apsvērumu dēļ dalībvalstis var izņēmuma kārtā atturēties ievadīt brīdinājumu, ja tas varētu traucēt oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras.

22. pants

Prasības brīdinājuma ievadīšanai

1. To datu minimuma kopums, kas vajadzīgi, lai ievadītu brīdinājumu *SIS*, ir dati, kas minēti 20. panta 3. punkta a), g), k), un n) apakšpunktā, izņemot 40. pantā minētajās situācijās. *SIS* ievada arī citus minētajā punktā norādītos datus, ja tie ir pieejami.

2. Datus, kas minēti šīs regulas 20. panta 3. punkta e) apakšpunktā, ievada vienīgi tad, ja tas noteikti ir nepieciešams, lai varētu identificēt attiecīgo personu. Ja tiek ievadīti šādi dati, dalībvalstis nodrošina, ka tiek ievērots Direktīvas (ES) 2016/680 10. pants.

23. pants

Brīdinājumu savietojamība

1. Pirms brīdinājuma ievadīšanas dalībvalsts pārbauda, vai par attiecīgo personu vai priekšmetu *SIS* jau nav ievadīts brīdinājums. Lai pārbaudītu, vai par attiecīgo personu jau nav ievadīts brīdinājums, veic arī pārbaudi ar daktiloskopiskajiem datiem, ja šādi dati ir pieejami.

2. Par vienu personu vai vienu priekšmetu katra dalībvalsts *SIS* ievada tikai vienu brīdinājumu. Ja nepieciešams, jaunus brīdinājumus par to pašu personu vai priekšmetu var ievadīt citas dalībvalstis saskaņā ar 3. punktu.

3. Ja par kādu personu vai priekšmetu *SIS* jau ir ievadīts brīdinājums, tad dalībvalsts, kura grib ievadīt jaunu brīdinājumu, pārbauda, vai brīdinājumi nav nesavietojami. Ja nesavietojamību nekonstatē, dalībvalsts var ievadīt jauno brīdinājumu. Ja brīdinājumi nav savietojami, attiecīgie dalībvalstu *SIRENE* biroji papildinformācijas apmaiņas ceļā savstarpēji apspriežas, lai panāktu vienošanos. Noteikumus par brīdinājumu savietojamību paredz *SIRENE* rokasgrāmatā. Pēc apspriešanās starp dalībvalstīm un ja tiek apdraudētas būtiskas valsts intereses, var atkāpties no noteikumiem par savietojamību.

4. Ja ir konstatētas vairākas informācijas atbilsmes saistībā ar vairākiem brīdinājumiem par vienu un to pašu personu vai priekšmetu, izpildītāja dalībvalsts ievēro brīdinājumu prioritātes noteikumus, kas noteikti *SIRENE* rokasgrāmatā.

Ja uz personu attiecas vairāki brīdinājumi, kurus ievadījušas dažādas dalībvalstis, brīdinājumus par apcietināšanu, kas ievadīti saskaņā ar 26. pantu, izpilda prioritārā kārtā, ievērojot 25. pantu.

24. pants

Vispārīgi noteikumi par atzīmju pievienošanu brīdinājumiem

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

2. Lai dalībvalstīm dotu iespēju pieprasīt, ka atzīmi pievieno saskaņā ar 26. pantu ievadītam brīdinājumam, visām dalībvalstīm, veicot papildinformācijas apmaiņu, automātiski paziņo par jebkādu jaunu minētās kategorijas brīdinājumu.

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

25. pants

Atzīmju pievienošana brīdinājumiem par personu apcietināšanu nolūkā tās nodot

1. Ja uz gadījumu attiecas Pamatlēmums 2002/584/TI, dalībvalsts pieprasa izdevējai dalībvalstij kā pēcpasākumu brīdinājumam par personas apcietināšanu nolūkā to nodot, pievienot atzīmi par apcietināšanas nepieļaušanu, 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 pievienot brīdinājumam atzīmi.

   Dalībvalsts var arī pieprasīt, lai brīdinājumam pievieno atzīmi, ja tās kompetentā tiesu iestāde nodošanas procesa laikā atbrīvo brīdinājuma subjektu.

2. Tomēr pēc kompetentas tiesu iestādes lūguma atbilstīgi valsts tiesību aktiem – vai nu balstoties uz vispārēju instrukciju, vai kādā īpašā gadījumā – dalībvalsts var arī pieprasīt izdevējai dalībvalstij pievienot atzīmi brīdinājumam par personas apcietināšanu nolūkā to nodot, ja ir acīmredzams, ka Eiropas apcietināšanas ordera izpilde būs jāatsaka.

IV NODAĻA
BRĪDINĀJUMI PAR PERSONĀM, KO MEKLĒ, LAI TĀS APCIETINĀTU NOLŪKĀ TĀS NODOT VAI IZDOT

26. pants

Brīdinājumu ievadīšanas mērķi un nosacījumi

1. Brīdinājumus 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. Brīdinājumus, lai apcietinātu nolūkā personas nodot ievada arī pamatojoties uz apcietināšanas orderi, kas izdots atbilstīgi nolīgumiem, kuri saskaņā ar Līgumiem 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 Pamatlēmuma 2002/584/TI noteikumiem uzskata par atsauci arī uz atbilstošajiem noteikumiem nolīgumos, kas saskaņā ar Līgumiem noslēgti starp 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 operācijas gadījumā saskaņā ar šo pantu ievadītu brīdinājumu par apcietināšanu var uz laiku padarīt meklēšanai nepieejamu galalietotājiem dalībvalstīs, kas iesaistītas attiecīgajā operācijā. Šādos gadījumos brīdinājums ir pieejams tikai *SIRENE* birojiem. Dalībvalstis brīdinājumu padara nepieejamu tikai tad, ja:

   a) operācijas mērķi nevar sasniegt ar citiem pasākumiem;

   b) izdevējas dalībvalsts kompetentā tiesu iestāde ir piešķīrusi iepriekšēju atļauju; un

   c) visas dalībvalstis, kas iesaistītas operācijā, ir informētas papildinformācijas apmaiņas ceļā.

   Funkciju, kas minēta pirmajā daļā, izmanto tikai uz laiku, kas nepārsniedz 48 stundas. Tomēr operatīvos nolūkos to var pagarināt vēl par 48 stundām. Dalībvalstis glabā statistiku par to brīdinājumu skaitu, saistībā ar kuriem šī funkcija ir izmantota.

5. Ja ir skaidra norāde, ka priekšmeti, kas minēti 38. panta 2. punkta a), b), c), e), g), h), j) un k) apakšpunktā, ir saistīti ar personu, uz kuru attiecas brīdinājums, ievērojot šā panta 1. un 2. punktu, par minētajiem priekšmetiem var ievadīt brīdinājumus, lai atrastu personu. Šādos gadījumos brīdinājumu par personu un brīdinājumu par priekšmetu sasaista saskaņā ar 63. pantu.

6. Komisija pieņem īstenošanas aktus, lai noteiktu un pilnveidotu noteikumus, kas nepieciešami, lai ievadītu, atjauninātu, dzēstu un meklētu datus, kas minēti šā panta 5. punktā. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

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.

   Dalībvalsts brīdinājumā par personas apcietināšanu nolūkā to nodot var ievadīt vairāk kā viena Eiropas apcietināšanas ordera kopiju.

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

28. pants

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

Brīdinājuma par personas apcietināšanu nolūkā to nodot izdevēja dalībvalsts paziņo Pamatlēmuma 2002/584/TI 8. panta 1. punktā minēto informāciju pārējām dalībvalstīm, veicot papildinformācijas apmaiņu.

29. pants

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

1. Brīdinājuma par personas apcietināšanu nolūkā to izdot izdevēja dalībvalsts, veicot papildinformācijas apmaiņu, visām citām 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 ievadīts brīdinājums;

   e) ja iespējams, noziedzīgā nodarījuma sekas; un

   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 izpildītāja dalībvalsts varētu izpildīt brīdinājumu.

30. pants

Rīcības, kas jāveic attiecībā uz brīdinājumiem par personas apcietināšanu nolūkā to nodot vai izdot, pārveidošana

Ja apcietināšanu nav iespējams izdarīt – vai nu tāpēc, ka dalībvalsts, kurai tas lūgts, atsakās to darīt saskaņā ar 24. vai 25. pantā izklāstītajām procedūrām par atzīmju pievienošanu, vai arī tāpēc, ka attiecībā uz brīdinājumu par personas apcietināšanu nolūkā to izdot vēl nav pabeigta izmeklēšana –, tad dalībvalsts, kam lūgts izdarīt apcietināšanu, rīkojas saistībā ar brīdinājumu, paziņojot attiecīgās personas atrašanās vietu.

31. pants

Rīcības, kas pamatota uz brīdinājumu par personas apcietināšanu nolūkā to nodot vai izdot, izpilde

1. Ja ir piemērojams Pamatlēmums 2002/584/TI, tad saskaņā ar 26. pantu *SIS* ievadītu brīdinājumu un 27. pantā minētos papildu datus kopā 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 VAI NEAIZSARGĀTĀM PERSONĀM, KAM JĀLIEDZ CEĻOT

32. pants

Brīdinājumu ievadīšanas mērķi un nosacījumi

1. Pēc izdevējas dalībvalsts kompetentās iestādes lūguma *SIS* ievada brīdinājumus par šādu kategoriju personām:

a) pazudušas personas, kas jāaizsargā:

i) viņu pašu aizsardzībai;

ii) lai novērstu sabiedriskās kārtības vai sabiedriskās drošības apdraudējumu;

b) pazudušas personas, kas nav jāaizsargā;

c) viena no vecākiem, ģimenes locekļa vai aizbildņa veiktas nolaupīšanas riskam pakļauti bērni, kuriem jāliedz ceļot;

d) bērni, kuriem jāliedz ceļot un attiecībā uz kuriem pastāv konkrēts un acīmredzams risks, ka tos var aizvest no dalībvalsts teritorijas vai viņi var to atstāt un

i) kļūt par cietušajiem cilvēku tirdzniecībā vai saistībā ar piespiedu laulību, sieviešu dzimumorgānu kropļošanu vai citiem ar dzimumu saistītas vardarbības veidiem,

ii) kļūt par cietušajiem vai tikt iesaistīti teroristu nodarījumos, vai

iii) tikt iesaukti vai iesaistīti bruņotās grupās vai kuriem var likt aktīvi piedalīties karadarbībā;

e) pilngadīgas neaizsargātas personas, kurām jāliedz ceļot viņu pašu aizsardzības dēļ un attiecībā uz kuriem pastāv konkrēts un acīmredzams risks, ka tās var aizvest no dalībvalsts teritorijas vai viņas var to atstāt un kļūt par cietušajiem cilvēku tirdzniecībā vai ar dzimumu saistītā vardarbībā.

2. Šā panta 1. punkta a) apakšpunktu piemēro vienīgi bērniem un personām, kuras saskaņā ar kompetentas iestādes lēmumu ir jāievieto iestādē.

3. Brīdinājumu par bērnu, kas minēts 1. punkta c) apakšpunktā, ievada pēc kompetento iestāžu, tostarp dalībvalstu tiesu iestāžu, kurām ir jurisdikcija lietās par vecāku atbildību, lēmuma, ja pastāv konkrēts un acīmredzams risks, ka bērnu var nelikumīgi un nenovēršami aizvest no dalībvalsts, kurā atrodas kompetentās iestādes.

4. Brīdinājumu par personām, kas minētas 1. punkta d) un e) apakšpunktā, ievada pēc kompetento iestāžu, tostarp tiesu iestāžu, lēmuma.

5. Izdevēja dalībvalsts regulāri pārskata nepieciešamību saglabāt šā panta 1. panta c), d) un e) apakšpunktā minētos brīdinājumus saskaņā ar 53. panta 4. punktu.

6. Izdevēja dalībvalsts nodrošina visu turpmāk minēto:

a) ka dati, ko tā ievada *SIS*, norāda, pie kuras no 1. punktā minētajām kategorijām pieder persona, uz kuru attiecas brīdinājums.

b) ka dati, ko tā ievada *SIS*, norāda, kāda veida gadījums ir iesaistīts, ja gadījuma veids ir zināms; un

c) ka attiecībā uz brīdinājumiem, kas ievadīti saskaņā ar 1. punkta c), d) un e) apakšpunktu, tās *SIRENE* biroja rīcībā ir visa attiecīgā informācija brīdinājuma izveides laikā.

7. Četrus mēnešus pirms tam, kad bērns, uz kuru attiecas brīdinājums saskaņā ar šo pantu, ir sasniedzis pilngadību saskaņā ar izdevējas dalībvalsts valsts tiesību aktiem, *CS-SIS* automātiski informē izdevēju dalībvalsti, ka vai nu ir jāatjaunina brīdinājuma un veicamās darbības pamats, vai arī brīdinājums ir jādzēš.

8. Ja ir skaidra norāde, ka priekšmeti, kas minēti 38. panta 2. punkta a), b), c), e), g), h) un k) apakšpunktā, ir saistīti ar personu, uz kuru attiecas brīdinājums, ievērojot šā panta 1. punktu, par minētajiem priekšmetiem var ievadīt brīdinājumus, lai atrastu personu. Šādos gadījumos brīdinājumu par personu un brīdinājumu par priekšmetu sasaista saskaņā ar 63. pantu.

9. Komisija pieņem īstenošanas aktus, lai noteiktu un pilnveidotu noteikumus par gadījumu veidu klasifikāciju un 6. punktā minēto datu ievadīšanu. Pazudušu personu, kas ir bērni, gadījumu veidi cita starpā – bet ne tikai – ietver aizbēgušus bērnus, nepavadītus bērnus ar migrāciju saistītos apstākļos un vecāku veiktas nolaupīšanas riskam pakļautus bērnus.

Komisija pieņem arī īstenošanas aktus, lai noteiktu un pilnveidotu tehniskos noteikumus, kas nepieciešami, lai ievadītu, atjauninātu, dzēstu un meklētu datus, kas minēti 8. punktā.

Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

33. pants

Rīcība, pamatojoties uz brīdinājumu

1. Ja konstatē 32. pantā minētās personas atrašanās vietu, izpildītājas dalībvalsts kompetentās iestādes, ievērojot šā panta 4. punktā izklāstītās prasības, paziņo šīs personas atrašanās vietu izdevējai dalībvalstij.

2. Attiecībā uz 32. panta 1. punkta a), c), d) un e) apakšpunktā minētajām personām, kas jāaizsargā, izpildītāja dalībvalsts papildinformācijas apmaiņas ceļā nekavējoties apspriežas ar savām un izdevējas dalībvalsts kompetentajām iestādēm, lai nekavējoties vienotos par veicamajiem pasākumiem. Izpildītājas dalībvalsts kompetentās iestādes saskaņā ar valsts tiesību aktiem var šādas personas nogādāt drošībā, lai tām neļautu turpināt ceļojumu.

3. Attiecībā uz bērniem jebkuru lēmumu par veicamajiem pasākumiem vai lēmumu nogādāt bērnu drošībā, kā minēts 2. punktā, pieņem, ievērojot bērna intereses. Šādu lēmumu pieņem nekavējoties, bet ne vēlāk kā 12 stundas pēc tam, kad konstatēta bērna atrašanās vieta, vajadzības gadījumā apspriežoties ar attiecīgajām bērnu aizsardzības iestādēm.

4. 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 personai, kas ziņoja par personas pazušanu, paziņot par brīdinājuma dzēšanu sakarā ar to, ka pazudusī persona ir atrasta.

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

34. pants

Brīdinājumu ievadīšanas mērķi un nosacījumi

1. Lai darītu zināmu personu uzturēšanās vietu vai pastāvīgo dzīvesvietu, dalībvalstis pēc kompetentas iestādes lūguma ievada *SIS* brīdinājumus par:

   a) lieciniekiem;

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

c) personām, kurām jāizsniedz spriedums kriminālllietā vai citi dokumenti saistībā ar krimināltiesvedību, 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 priekšmeti, kas minēti 38. panta 2. punkta a), b), c), e), g), h) un k) apakšpunktā, ir saistīti ar personu, uz kuru attiecas brīdinājums, ievērojot šā panta 1. punktu, par minētajiem priekšmetiem var ievadīt brīdinājumus, lai atrastu personu. Šādos gadījumos brīdinājumu par personu un brīdinājumu par priekšmetu sasaista saskaņā ar 63. pantu.

3. Komisija pieņem īstenošanas aktus, lai noteiktu un pilnveidotu tehniskos noteikumus, kas nepieciešami, lai ievadītu, atjauninātu, dzēstu un meklētu datus, kas minēti šā panta 2. punktā. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

35. pants

Rīcība, pamatojoties uz brīdinājumu

Pieprasīto informāciju dara zināmu izdevējai dalībvalstij, veicot papildinformācijas apmaiņu.

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

36. pants

Brīdinājumu ievadīšanas mērķi un nosacījumi

1. Lai nodrošinātu diskrētas pārbaudes, izmeklēšanas pārbaudes vai īpašas pārbaudes saskaņā ar 37. panta 3., 4. un 5. punktu, brīdinājumus par personām, par priekšmetiem, kas minēti 38. panta 2. punkta a), b), c), e), g), h), j), k) un l) apakšpunktā, un par bezskaidras naudas maksāšanas līdzekļiem ievada saskaņā ar izdevējas dalībvalsts tiesību aktiem.

2. Ievadot brīdinājumus par diskrētām pārbaudēm, izmeklēšanas pārbaudēm vai īpašām pārbaudēm, un ja informācija, ko lūdz izdevēja dalībvalsts, ir papildus tai informācijai, kas paredzēta 37. panta 1. punkta a)–h) apakšpunktā, izdevēja dalībvalsts pievieno brīdinājumam visu informāciju, kas tiek lūgta. Ja minētā informācija attiecas uz īpašu kategoriju personas datiem, kas minēti Direktīvas (ES) 2016/680 10. pantā, to lūdz tikai tad, ja tas ir noteikti nepieciešams konkrētajam brīdinājuma mērķim un saistībā ar noziedzīgo nodarījumu, par kuru ievadīts brīdinājums.

3. Brīdinājumus par personām saistībā ar diskrētām pārbaudēm, izmeklēšanas pārbaudēm vai īpašām pārbaudēm var ievadīt, lai novērstu, atklātu, izmeklētu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, izpildītu kriminālsodu un novērstu sabiedriskās drošības apdraudējumus vienā vai vairākos šādos apstākļos:

   a) ja ir skaidra norāde, ka attiecīgā persona ir nodomājusi izdarīt vai izdara kādu no Pamatlēmuma 2002/584/TI 2. panta 1. un 2. punktā minētajiem nodarījumiem;

   b) ja 37. panta 1. punktā minētā informācija ir nepieciešama, lai izpildītu brīvības atņemšanas sodu vai ar brīvības atņemšanu saistītu drošības līdzekli personai, kas notiesāta par kādu no Pamatlēmuma 2002/584/TI 2. panta 1. un 2. punktā minētajiem nodarījumiem;

   c) ja vispārējs personas novērtējums, īpaši ņemot vērā līdz šim izdarītos noziedzīgos nodarījumus, ļauj uzskatīt, ka minētā persona nākotnē var izdarīt Pamatlēmuma 2002/584/TI 2. panta 1. un 2. punktā minētos nodarījumus.

4. Turklāt saskaņā ar attiecīgās valsts tiesību aktiem brīdinājumus par personām saistībā ar diskrētām pārbaudēm, izmeklēšanas pārbaudēm vai īpašām pārbaudēm var ievadīt 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 nopietnu apdraudējumu, ko rada attiecīgā persona, vai citus nopietnus valsts iekšējās vai ārējās drošības apdraudējumus. Dalībvalsts, kas ievadījusi brīdinājumu saskaņā ar šo punktu, par šādu brīdinājumu informē pārējās dalībvalstis. Katra dalībvalsts nosaka, kurām iestādēm nosūta šo informāciju. Informāciju nosūta ar *SIRENE* biroju starpniecību.

5. Ja ir skaidra norāde, ka priekšmeti, kas minēti 38. panta 2. punkta a), b), c), e), g), h), j), k) un l) apakšpunktā, vai bezskaidras naudas maksāšanas līdzekļi ir saistīti ar smagiem noziegumiem, kas minēti šā panta 3. punktā, vai nopietniem apdraudējumiem, kas minēti šā panta 4. punktā, par minētajiem priekšmetiem var ievadīt brīdinājumus, un tos sasaistīt ar brīdinājumiem, kas ievadīti saskaņā ar šā panta 3. un 4. punktu.

6. Komisija pieņem īstenošanas aktus, lai noteiktu un pilnveidotu tehniskos noteikumus, kas nepieciešami, lai ievadītu, atjauninātu, dzēstu un meklētu datus, kas minēti šā panta 5. punktā, kā arī papildu informāciju, kas minēta šā panta 2. punktā. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

37. pants

Rīcība, pamatojoties uz brīdinājumu

1. Lai veiktu diskrētas pārbaudes, izmeklēšanas pārbaudes vai īpašas pārbaudes, izpildītāja dalībvalsts vāc un paziņo izdevējai dalībvalstij visu turpmāk norādīto informāciju vai tās daļu:

a) tas, ka ir atrasta persona, uz kuru attiecas brīdinājums, vai ka ir atrasti priekšmeti, kas minēti 38. panta 2. punkta a), b), c), e), g), h), j), k) un l) apakšpunktā, vai bezskaidras naudas maksāšanas līdzekļi, uz kuriem attiecas brīdinājums;

b) pārbaudes vieta, laiks un iemesls;

c) ceļojuma maršruts un galamērķis;

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

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

f) priekšmeti, kas minēti 38. panta 2. punkta a), b), c), e), g), h), j), k) un l) apakšpunktā, vai bezskaidras naudas maksāšanas līdzekļi, kas izmantoti;

g) transportētie priekšmeti, tostarp ceļošanas dokumenti;

h) apstākļi, kādos persona, priekšmeti, kas minēti 38. panta 2. punkta a), b), c), e), g), h), j), k) un l) apakšpunktā, vai bezskaidras naudas maksāšanas līdzekļi tika atrasti;

i) jebkāda cita informācija, ko lūdz izdevēja dalībvalsts saskaņā ar 36. panta 2. punktu.

Ja informācija, kas minēta šā punkta pirmās daļas i) apakšpunktā, attiecas uz īpašu kategoriju personas datiem, kas minēti Direktīvas (ES) 2016/680 10. pantā, to apstrādā saskaņā ar minētajā pantā izklāstītajiem nosacījumiem un tikai tad, ja tā papildina citus personas datus, ko apstrādā tam pašam mērķim.

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

3. Diskrēta pārbaude ietver to, ka izpildītājas dalībvalsts valsts kompetento iestāžu veikto regulāro darbību laikā diskrēti tiek vākts, cik vien iespējams, daudz 1. punktā aprakstītās informācijas. Šīs informācijas vākšana neapdraud pārbaužu diskrētumu, un brīdinājuma subjektam nekādā veidā nedara zināmu to, ka šāds brīdinājums pastāv.

4. Izmeklēšanas pārbaude ietver personas interviju, tostarp, pamatojoties uz informāciju vai konkrētiem jautājumiem, ko brīdinājumam pievienojusi izdevēja dalībvalsts saskaņā ar 36. panta 2. punktu. Interviju veic saskaņā ar izpildītājas dalībvalsts valsts tiesību aktiem.

5. Veicot īpašās pārbaudes, 36. pantā minētajos nolūkos var pārmeklēt personas, transportlīdzekļus, laivas, gaisa kuģus, konteinerus un transportējamos priekšmetus. Pārmeklēšanu īsteno saskaņā ar izpildītājas dalībvalsts tiesību aktiem.

6. Ja saskaņā ar izpildītājas dalībvalsts tiesību aktiem īpašās pārbaudes nav atļautas, šajā dalībvalstī tās aizstāj ar izmeklēšanas pārbaudēm. Ja saskaņā ar izpildītājas dalībvalsts tiesību aktiem izmeklēšanas pārbaudes nav atļautas, šajā dalībvalstī tās aizstāj ar diskrētām pārbaudēm. Ja piemēro Direktīvu 2013/48/ES, dalībvalstis nodrošina, lai tiktu ievērotas aizdomās turēto un apsūdzēto personu tiesības uz advokāta palīdzību saskaņā ar nosacījumiem, kas izklāstīti minētajā direktīvā.

7. Šā panta 6. punkts neskar dalībvalstu pienākumu galalietotājiem darīt pieejamu informāciju, ko lūdz saskaņā ar 36. panta 2. punktu.

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

38. pants

Brīdinājumu ievadīšanas mērķi un nosacījumi

1. Dalībvalstis ievada *SIS* brīdinājumus par priekšmetiem, ko meklē, lai izņemtu vai izmantotu par pierādījumu kriminālprocesā.

2. Brīdinājumus ievada par šādām viegli identificējamu priekšmetu kategorijām:

a) mehāniskie transportlīdzekļi 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) gaisa kuģu dzinēji;

j) šaujamieroči;

k) nozagtas, nelikumīgi piesavinātas, pazudušas oficiālu dokumentu veidlapas vai tādas oficiālu dokumentu veidlapas, kas, būdamas neīstas, tiek uzdotas par īstām;

l) izsniegti personu apliecinoši dokumenti, kas nozagti, nelikumīgi piesavināti, pazuduši, atzīti par nederīgiem vai, būdami neīsti, tiek uzdoti par īstiem, piemēram, pases, personas apliecības, uzturēšanās atļaujas, ceļošanas dokumenti, kā arī transportlīdzekļa vadītāja apliecības;

m) transportlīdzekļu reģistrācijas apliecības un transportlīdzekļa numura zīmes, kas nozagtas, nelikumīgi piesavinātas, pazudušas vai atzītas par nederīgām vai, būdamas neīstas, tiek uzdotas par īstām;

n) banknotes (reģistrētas naudaszīmes) un viltotas banknotes;

o) informācijas tehnoloģiju vienības;

p) identificējamas mehānisko transportlīdzekļu detaļas;

q) identificējamas rūpniecības iekārtu detaļas;

r) citi identificējami augstvērtīgi priekšmeti, kā noteikts saskaņā ar 3. punktu.

Attiecībā uz dokumentiem, kas minēti k), l) un m) apakšpunktā, izdevēja dalībvalsts var precizēt, vai šādi dokumenti ir nozagti, nelikumīgi piesavināti, pazuduši, atzīti par nederīgiem vai neīsti.

3. Komisija tiek pilnvarota saskaņā ar 75. pantu pieņemt deleģētos aktus, lai grozītu šo regulu, definējot jaunas to priekšmetu apakškategorijas, kuri minēti šā panta 2. punkta o), p), q) un r) apakšpunktā.

4. Komisija pieņem īstenošanas aktus, lai noteiktu un izstrādātu tehniskos noteikumus, kas vajadzīgi šā panta 2. punktā minēto datu ievadīšanai, atjaunināšanai, dzēšanai un meklēšanai. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

39. pants

Rīcība, pamatojoties uz brīdinājumu

1. Ja meklēšanā konstatē brīdinājumu par atrastu priekšmetu, tad kompetentā iestāde saskaņā ar valsts tiesību aktiem izņem priekšmetu un sazinās ar izdevējas dalībvalsts 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. Izpildītāja dalībvalsts veic prasītos pasākumus saskaņā ar saviem tiesību aktiem.

XI NODAĻA
BRĪDINĀJUMI PAR NEZINĀMĀM MEKLĒTĀM PERSONĀM IDENTIFIKĀCIJAS NOLŪKĀ SASKAŅĀ AR VALSTS TIESĪBU AKTIEM

40. pants

Brīdinājumi par nezināmām meklētām personām identifikācijas nolūkā saskaņā ar valsts tiesību aktiem

Dalībvalstis *SIS* var ievadīt brīdinājumus par nezināmām meklētām personām, kuri satur tikai daktiloskopiskos datus. Minētie daktiloskopiskie dati ir vai nu pilni vai nepilni pirkstu nospiedumu vai plaukstu nospiedumu komplekti, kas konstatēti izmeklējamu teroristu nodarījumu vai citu smagu noziegumu izdarīšanas vietās. Tos ievada *SIS* tikai tad, ja ar ļoti augstu varbūtības pakāpi var konstatēt, ka tie pieder nodarījuma izdarītājam.

Ja izdevējas dalībvalsts kompetentā iestāde nevar noteikt aizdomās turētā identitāti, pamatojoties uz jebkuras citas attiecīgas valsts, Savienības vai starptautiskas datubāzes datiem, pirmajā daļā minētos daktiloskopiskos datus šajā brīdinājumu kategorijā var ievadīt tikai kā "nezināma meklēta persona" šādas personas identificēšanas nolūkā.

41. pants

Rīcība, pamatojoties uz brīdinājumu

Ja ir konstatēta informācijas atbilsme ar datiem, kas ievadīti, ievērojot 40. pantu, personas identitāti nosaka saskaņā ar valsts tiesību aktiem, vienlaikus ekspertam pārliecinoties, ka *SIS* daktiloskopiskie dati pieder šai personai. Izpildītājas dalībvalstis paziņo informāciju par personas identitāti un atrašanās vietu izdevējai dalībvalstij, izmantojot papildinformācijas apmaiņu, lai atvieglotu savlaicīgu lietas izmeklēšanu.

XII NODAĻA
ĪPAŠI NOTEIKUMI BIOMETRISKAJIEM DATIEM

42. pants

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

1. *SIS* ievada tikai fotogrāfijas, sejas attēlus, daktiloskopiskos datus, kas minēti 20. panta 3. punkta w) un y) apakšpunktā un kas atbilst minimālajiem datu kvalitātes standartiem un tehniskajām specifikācijām. Pirms šādu datu ievadīšanas veic kvalitātes pārbaudi, lai pārliecinātos, vai ir nodrošināta atbilstība minimālajiem datu kvalitātes standartiem un tehniskajām specifikācijām.

2. *SIS* ievadītie daktiloskopiskie dati var sastāvēt no viena līdz desmit pirkstu nospiedumiem, kas iegūti ar uzspiešanas metodi, un no viena līdz desmit pirkstu nospiedumiem, kas iegūti ar pārvelšanas metodi. Tajos var iekļaut arī līdz diviem plaukstu nospiedumiem.

3. DNS profilu var pievienot brīdinājumiem tikai 32. panta 1. punkta a) apakšpunktā paredzētajās situācijās tikai pēc kvalitātes pārbaudes, kurā pārliecinās, vai ir nodrošināta atbilstība minimālajiem datu kvalitātes standartiem un tehniskajām specifikācijām, un tikai tad, ja fotogrāfijas, sejas attēli vai daktiloskopiskie dati nav pieejami vai nav piemēroti identifikācijai. Tādu personu DNS profilus, kas ir brīdinājuma subjekta tiešie augšupējie radinieki, pēcnācēji, brāļi vai māsas, var pievienot brīdinājumam ar noteikumu, ka minētās personas dod savu nepārprotamu piekrišanu. Ja brīdinājumam pievieno DNS profilu, minētajā profilā iekļauj tikai minimālo informāciju, kas ir noteikti nepieciešama pazudušas personas identifikācijai.

4. Šā panta 1. un 3. punktā minēto biometrisko datu glabāšanai saskaņā ar šā panta 5. punktu nosaka minimālos datu kvalitātes standartus un tehniskās specifikācijas. Minētie minimālie datu kvalitātes standarti un tehniskās specifikācijas nosaka kvalitātes līmeni, kas nepieciešams datu izmantošanai, lai pārbaudītu personas identitāti saskaņā ar 43. panta 1. punktu, un datu izmantošanai, lai identificētu personu saskaņā ar 43. panta 2.–4. punktu.

5. Komisija pieņem īstenošanas aktus, lai noteiktu šā panta 1., 3. un 4. punktā minētos minimālos datu kvalitātes standartus un tehniskās specifikācijas. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

43. pants

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

1. Ja *SIS* brīdinājumā ir pieejamas fotogrāfijas, sejas attēli, daktiloskopiskie dati un DNS profili, šādas fotogrāfijas, sejas attēlus, daktiloskopiskos datus un DNS profilus izmanto, lai apstiprinātu tādas personas identitāti, kura ir atrasta *SIS* burtciparu meklēšanas rezultātā.

2. Lai identificētu personu, visos gadījumos var veikt meklēšanu daktiloskopiskajos datos. Tomēr, ja personas identitāti nevar noskaidrot, izmantojot citus līdzekļus, lai identificētu personu veic meklēšanu daktiloskopiskajos datos. Minētajā nolūkā centrālā *SIS* ietver automatizētu pirkstu nospiedumu identifikācijas sistēmu (*AFIS*).

3. Daktiloskopiskajos datos *SIS* saistībā ar brīdinājumiem, kuri ievadīti saskaņā ar 26., 32., 36. un 40. pantu, var meklēt arī, izmantojot pilnus vai nepilnus tādu pirkstu nospiedumu vai plaukstu nospiedumu komplektus, kuri konstatēti izmeklējamu smagu noziegumu vai teroristu nodarījumu izdarīšanas vietās, ja ar augstu varbūtības pakāpi var konstatēt, ka minētie nospiedumu komplekti pieder nodarījuma izdarītājam, un ar noteikumu, ka meklēšanu veic vienlaikus dalībvalsts attiecīgajās valstu pirkstu nospiedumu datubāzēs.

4. Tiklīdz tas ir tehniski iespējams un vienlaikus identifikācijai nodrošinot augstu uzticamības pakāpi, fotogrāfijas un sejas attēlus var izmantot personas identifikācijai saistībā ar regulārajām robežšķērsošanas vietām.

Pirms šo funkciju ievieš *SIS*, Komisija sniedz ziņojumu par vajadzīgās tehnoloģijas pieejamību, par to, vai tā spēj pareizi darboties, un par tās uzticamību. Par ziņojumu apspriežas ar Eiropas Parlamentu.

Pēc tam, kad ir sākta šīs funkcijas izmantošana regulārajās robežšķērsošanas vietās, Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 75. pantu, lai papildinātu šo regulu attiecībā uz citu apstākļu noteikšanu, kādos fotogrāfijas un sejas attēlus var izmantot personu identifikācijai.

XIII NODAĻA
PIEKĻUVES TIESĪBAS UN BRĪDINĀJUMU PĀRSKATĪŠANA

44. pants

Valsts kompetentās iestādes, kurām ir tiesības piekļūt SIS datiem

1. Valsts kompetentajām iestādēm ir piekļuve *SIS* ievadītajiem datiem un tiesības veikt tiešu meklēšanu šādos datos vai *SIS* datubāzes kopijā, lai:

   a) veiktu robežkontroli saskaņā ar Regulu (ES) 2016/399,

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

   c) attiecīgajā dalībvalstī novērstu, atklātu, izmeklētu teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, ar noteikumu, ka tiek piemērota Direktīva (ES) 2016/680;

d) izpētītu nosacījumus un pieņemtu lēmumus, kas saistīti ar trešo valstu valstspiederīgo ieceļošanu un uzturēšanos dalībvalstu teritorijā, tostarp attiecībā uz uzturēšanās atļaujām un ilgtermiņa vīzām, un ar trešo valstu valstspiederīgo atgriešanu, kā arī veiktu to trešo valstu valstspiederīgo pārbaudes, kuri nelikumīgi ieceļo vai uzturas dalībvalstu teritorijā;

e) veiktu to trešo valstu valstspiederīgo drošības pārbaudes, kuri piesakās uz starptautisko aizsardzību, tiktāl, ciktāl iestādes, kas veic pārbaudes, nav "atbildīgās iestādes", kā definēts Eiropas Parlamenta un Padomes Direktīvas 2013/32/ES[1] 2. panta f) punktā, un vajadzības gadījumā sniedzot konsultācijas saskaņā ar Padomes Regulu (EK) Nr. 377/2004[2].

2. Tiesības piekļūt *SIS* datiem un tiesības veikt tiešu meklēšanu šādos datos var būt par naturalizāciju atbildīgajām valsts kompetentajām iestādēm, kā paredzēts valsts tiesību aktos, naturalizācijas pieteikuma izskatīšanas nolūkos.

3. 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 personai – pildot attiecīgās valsts tiesību aktos paredzētos uzdevumus, kā arī šādu iestāžu darbības koordinēšanas iestādēm.

---

[1] Eiropas Parlamenta un Padomes Direktīva 2013/32/ES (2013. gada 26. jūnijs) par kopējām procedūrām starptautiskās aizsardzības statusa piešķiršanai un atņemšanai (OV L 180, 29.6.2013., 60. lpp.).

[2] Padomes Regula (EK) Nr. 377/2004 (2004. gada 19. februāris) par sadarbības koordinatoru tīkla izveidi imigrācijas jomā (OV L 64, 2.3.2004., 1. lpp.).

4. Šajā pantā minētās kompetentās iestādes iekļauj 56. panta 7. punktā minētajā sarakstā.

45. pants

Transportlīdzekļu reģistrācijas dienesti

1. Dalībvalstu dienestiem, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izdošanu, kā minēts Padomes Direktīvā 1999/37/EK[1], ir piekļuve datiem, kas ievadīti *SIS* saskaņā ar šīs regulas 38. panta 2. punkta a), b), c), m) un p) apakšpunktu, vienīgi nolūkā pārbaudīt, vai tām reģistrācijai pieteiktie transportlīdzekļi un pievienotās transportlīdzekļu reģistrācijas apliecības un numura zīmes nav zagtas, nelikumīgi piesavinātas, pazaudētas, būdamas neīstas, netiek uzdotas par īstām, vai netiek meklētas kā pierādījums kriminālprocesā.

   Šā punkta pirmajā daļā minēto dienestu piekļuvi datiem reglamentē valsts tiesību akti, un to ierobežo attiecīgo dienestu īpašā kompetence.

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

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

3. Šā panta 1. punktā minētajiem dienestiem, kas nav valdības dienesti, ir tiesības piekļūt *SIS* datiem vienīgi ar 44. pantā minētas iestādes starpniecību. Minētajai iestādei ir tiesības tieši piekļūt datiem un nodot tos attiecīgajam dienestam. Attiecīgā dalībvalsts nodrošina, lai atbilstīgajam dienestam un tā darbiniekiem tiktu izvirzīta prasība ievērot jebkādus ierobežojumus pieļaujamā to datu izmantošanā, kurus tiem sniegusi iestāde.

4. Šīs regulas 39. pantu nepiemēro piekļuvei *SIS*, kas iegūta saskaņā ar šo pantu. Ja šā panta 1. punktā minētie dienesti, piekļūstot *SIS*, iegūst informāciju, šādas informācijas paziņošanu policijai vai tiesu iestādēm reglamentē attiecīgās valsts tiesību akti.

46. pants

Laivu un gaisa kuģu reģistrācijas dienesti

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

   a) dati par laivām;

   b) dati par laivu dzinējiem;

c) dati par gaisa kuģiem;

d) dati par gaisa kuģu dzinējiem.

Šā punkta pirmajā daļā minēto dienestu piekļuvi datiem reglamentē valsts tiesību akti, un to ierobežo attiecīgo dienestu īpašā kompetence.

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

3. Šā panta 1. punktā minētajiem dienestiem, kas nav valdības dienesti, ir tiesības piekļūt *SIS* datiem vienīgi ar 44. pantā minētas iestādes starpniecību. Minētajai iestādei ir tiesības tieši piekļūt datiem un nodot tos attiecīgajam dienestam. Attiecīgā dalībvalsts nodrošina, lai atbilstīgajam dienestam un tā darbiniekiem tiktu izvirzīta prasība ievērot jebkādus ierobežojumus pieļaujamā to datu izmantošanā, kurus tiem sniegusi iestāde.

4. Šīs regulas 39. pantu nepiemēro piekļuvei *SIS*, kas iegūta saskaņā ar šo pantu. Ja šā panta 1. punktā minētie dienesti, piekļūstot *SIS*, iegūst informāciju, šādas informācijas paziņošanu policijai vai tiesu iestādēm reglamentē attiecīgās valsts tiesību akti.

47. pants

Šaujamieroču reģistrācijas iestādes

1. Dalībvalstu dienestiem, kas ir atbildīgi par šaujamieroču reģistrācijas apliecību izdošanu, ir piekļuve saskaņā ar 26. un 36. pantu *SIS* ievadītiem datiem par personām un saskaņā ar 38. panta 2. punktu – *SIS* ievadītiem datiem par šaujamieročiem. Piekļuvi īsteno, lai pārbaudītu, vai persona, kas pieprasa reģistrāciju, tiek meklēta, lai to apcietinātu nodošanas vai izdošanas nolūkā vai diskrētas, izmeklēšanas vai īpašas pārbaudes nolūkā vai lai pārbaudītu, vai reģistrācijai pieteiktie šaujamieroči tiek meklēti, lai tos izņemtu vai izmantotu par pierādījumu kriminālprocesā.

2. Šā panta 1. punktā minēto dienestu piekļuvi datiem reglamentē valsts tiesību akti, un to ierobežo attiecīgo dienestu īpašā kompetence.

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

4. Šā panta 1. punktā minētajiem dienestiem, kas nav valdības dienesti, ir piekļuve tikai ar 44. pantā minētās iestādes starpniecību *SIS* datiem. Minētajai iestādei ir tiesības tieši piekļūt datiem, un tā informē attiecīgo dienestu par to, vai šaujamieroci var reģistrēt. Attiecīgā dalībvalsts nodrošina, lai attiecīgajam dienestam un tā darbiniekiem tiktu izvirzīta prasība ievērot jebkādus ierobežojumus pieļaujamā to datu izmantošanā, kurus tiem sniegusi starpniecības iestāde.

5. Šīs regulas 39. pantu nepiemēro piekļuvei *SIS*, kas iegūta saskaņā ar šo pantu. Ja šā panta 1. punktā minētie dienesti, piekļūstot *SIS*, iegūst informāciju, šādas informācijas paziņošanu policijai vai tiesu iestādēm reglamentē attiecīgās valsts tiesību akti.

48. pants

Eiropola piekļuve SIS *datiem*

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

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

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

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

5. Eiropols:

a) neskarot 4. un 6. punktu, nesasaista *SIS* daļas un nepārsūta tur esošos datus, kuriem tas var piekļūt, nevienai datu vākšanas un apstrādes sistēmai, ko ekspluatē Eiropols vai kas tiek ekspluatēta Eiropolā, kā arī neveic nekādas *SIS* daļas lejupielādi vai citādu kopēšanu;

b) neatkarīgi no Regulas (ES) 2016/794 31. panta 1. punkta dzēš papildinformāciju, kas satur personas datus, ne vēlāk kā vienu gadu pēc saistītā brīdinājuma dzēšanas. Atkāpjoties no šā noteikuma, ja Eiropolam tā datubāzēs vai operatīvās analīzes projektos ir informācija par gadījumu, ar kuru papildinformācija ir saistīta, lai Eiropols varētu veikt savus uzdevumus, Eiropols, ja vajadzīgs, izņēmuma kārtā var turpināt glabāt papildinformāciju. Eiropols informē izdevēju un izpildītāju dalībvalsti, ka šādu papildinformāciju turpina glabāt, un sniedz tam pamatojumu;

c) tiesības piekļūt *SIS* datiem, tostarp papildinformācijai, nodrošina vienīgi īpaši pilnvarotiem Eiropola darbiniekiem, kuriem piekļuve šādiem datiem nepieciešama viņu pienākumu pildīšanai;

d) pieņem un piemēro pasākumus ar mērķi nodrošināt drošību, konfidencialitāti un pašuzraudzību saskaņā ar 10., 11. un 13. pantu;

e) nodrošina, lai darbinieki, kam ir tiesības apstrādāt *SIS* datus, tiktu pienācīgi apmācīti un saņemtu informāciju saskaņā ar 14. panta 1. punktu; un

f) neskarot Regulu (ES) 2016/794, ļauj Eiropas Datu aizsardzības uzraudzītājam uzraudzīt un pārskatīt Eiropola darbības, ko tas veic, īstenojot tiesības piekļūt *SIS* datiem un meklēt tajos, un to, kā tas veic papildinformācijas apmaiņu un apstrādi.

6. Eiropols datus no *SIS* kopē vienīgi tehniskos nolūkos, ja šāda kopēšana ir vajadzīga, lai pienācīgi pilnvaroti Eiropola darbinieki varētu veikt tiešu meklēšanu šajos datos. Šādām kopijām piemēro šo regulu. Tehnisko kopiju izmanto vienīgi, lai saglabātu *SIS* datus, kamēr tajos notiek meklēšana. Tiklīdz meklēšana ir pabeigta, datus dzēš. Šādu izmantošanu neuzskata par *SIS* datu nelikumīgu lejupielādi vai kopēšanu. Eiropols nekopē brīdinājumu datus vai papildu datus, ko izdevušas dalībvalstis, vai datus no *CS-SIS* uz citām Eiropola sistēmām.

7. Lai pārbaudītu datu apstrādes likumību, veiktu pašuzraudzību un datiem nodrošinātu pienācīgu drošību un integritāti, Eiropols saglabā reģistra ierakstus par katru piekļuvi un meklēšanu *SIS* saskaņā ar 12. panta noteikumiem. Šādus reģistra ierakstus un dokumentus neuzskata par nelikumīgu kādas *SIS* daļas lejupielādi vai kopēšanu.

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

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

49. pants

Eurojust *piekļuve* SIS *datiem*

1. Tikai *Eurojust* valstu locekļiem un viņu asistentiem, ja tas vajadzīgs viņu pilnvaru izpildei, ir tiesības atbilstīgi viņu pilnvarām piekļūt *SIS* datiem un meklēt tajos saskaņā ar 26., 32., 34., 38. un 40. pantu.

2. Ja *Eurojust* valsts locekļa veiktā meklēšanā konstatē, ka *SIS* ir brīdinājums, minētais valsts loceklis informē izdevēju dalībvalsti. Šādā meklēšanā iegūtu informāciju *Eurojust* paziņo trešām valstīm un trešām struktūrām vienīgi ar izdevējas dalībvalsts piekrišanu un pilnībā ievērojot Savienības datu aizsardzības tiesību aktus.

3. Šis pants neskar Eiropas Parlamenta un Padomes Regulas (ES) 2018/…[1+] un Regulas (ES) 2018/…[++] noteikumus attiecībā uz datu aizsardzību un atbildību par jebkādu neatļautu vai nepareizu šādu datu apstrādi, ko veic *Eurojust* valstu locekļi vai viņu asistenti, un neskar Eiropas Datu aizsardzības uzraudzītāja pilnvaras, ievērojot minētās regulas.

4. Lai pārbaudītu datu apstrādes likumību, veiktu pašuzraudzību un datiem nodrošinātu pienācīgu drošību un integritāti, *Eurojust* saglabā reģistra ierakstus par katru piekļuvi un meklēšanu *SIS*, ko veic *Eurojust* valsts loceklis vai asistents saskaņā ar 12. panta noteikumiem.

5. Nevienu *SIS* daļu nepievieno nevienai datu vākšanas un apstrādes sistēmai, ko ekspluatē *Eurojust* vai kas tiek ekspluatēta *Eurojust*, un *SIS* datus, kuriem piekļūst valsts locekļi vai asistenti, nenosūta nevienai šādai sistēmai. *SIS* daļas netiek lejupielādētas vai kopētas. Reģistra ierakstu par piekļuvi un meklēšanu saglabāšanu neuzskata par *SIS* datu nelikumīgu lejupielādi vai kopēšanu.

6. *Eurojust* pieņem un piemēro pasākumus, ar ko nodrošina drošību, konfidencialitāti un pašuzraudzību saskaņā ar 10., 11. un 13. pantu.

---

1 Eiropas Parlamenta un Padomes Regula (ES) 2018/XXX (… gada …) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI (OV L...).

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 37/18 iekļautās regulas numuru un aizpildīt publikācijas atsauci zemsvītras piezīmē.

[++] OV: lūgums tekstā ievietot dokumentā PE-CONS 31/18 iekļautās regulas numuru.

50. 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 vienībām*

1. Saskaņā ar Regulas (ES) 2016/1624 40. panta 8. punktu minētās regulas 2. panta 8) un 9) punktā minēto vienību dalībniekiem atbilstīgi to pilnvarām un ar noteikumu, ka tie ir pilnvaroti veikt pārbaudes saskaņā ar šīs regulas 44. panta 1. punktu un tiem ir nodrošināta prasītā apmācība saskaņā ar šīs regulas 14. panta 1. punktu, ir tiesības piekļūt *SIS* datiem un meklēt tajos, ciktāl tas ir nepieciešams viņu pienākumu pildīšanai un ja to prasa konkrētās operācijas operatīvais plāns. Piekļuvi *SIS* datiem nepaplašina, attiecinot uz citiem vienības dalībniekiem.

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

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

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

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

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

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

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

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 31/18 izklāstītās regulas numuru.

51. pants

Izvērtējums par to, kā SIS izmanto Eiropols, Eurojust

un Eiropas Robežu un krasta apsardzes aģentūra

1. Komisija ne retāk kā reizi piecos gados izvērtē *SIS* darbību un to, kā Eiropols, *Eurojust* valstu locekļi un viņu asistenti un 50. panta 1. punktā minētās vienības to izmanto.

2. Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra nodrošina atbilstīgus pēcpasākumus saistībā ar konstatējumiem un ieteikumiem, kas izriet no izvērtējuma.

3. Ziņojumu par izvērtējuma rezultātiem un pēcpasākumiem nosūta Eiropas Parlamentam un Padomei.

52. pants

Piekļuves apjoms

Galalietotāji, tostarp Eiropols, *Eurojust* valstu locekļi un viņu asistenti un Regulas (ES) 2016/1624 2. panta 8) un 9) punktā minēto vienību dalībnieki piekļūst vienīgi tiem datiem, kas ir vajadzīgi to uzdevumu veikšanai.

53. pants

Pārskatīšanas periods brīdinājumiem par personām

1. Brīdinājumus par personām saglabā vienīgi tik ilgi, cik vajadzīgs, lai sasniegtu mērķus, kādiem tie ievadīti.

2. Dalībvalsts 26. panta un 32. panta 1. punkta a) un b) apakšpunkta nolūkos brīdinājumu par personu var ievadīt uz pieciem gadiem. Izdevēja dalībvalsts piecu gadu laikā pārskata nepieciešamību saglabāt brīdinājumu.

3. Dalībvalsts 34. un 40. panta nolūkos brīdinājumu par personu var ievadīt uz trīs gadiem. Izdevēja dalībvalsts trīs gadu laikā pārskata nepieciešamību saglabāt brīdinājumu.

4. Dalībvalsts 32. panta 1. punkta c), d) un e) apakšpunkta un 36. panta nolūkos brīdinājumu par personu var ievadīt uz vienu gadu. Izdevēja dalībvalsts viena gada laikā pārskata nepieciešamību saglabāt brīdinājumu.

5. Ikviena dalībvalsts vajadzības gadījumā saskaņā ar saviem tiesību aktiem nosaka īsākus pārskatīšanas termiņus.

6. Šā panta 2., 3. un 4. punktā minētajā pārskatīšanas periodā izdevēja dalībvalsts pēc visaptveroša individuāla novērtējuma, ko dokumentē, var pieņemt lēmumu brīdinājumu par personu saglabāt ilgāk par pārskatīšanas periodu, ja tas ir nepieciešami un samērīgi nolūkos, kādos brīdinājums ievadīts. Šādos gadījumos 2., 3. vai 4. punkts attiecas arī uz perioda pagarinājumu. Par jebkādu šādu pagarināšanu paziņo *CS-SIS*.

7. Brīdinājumus par personām automātiski dzēš, tiklīdz ir beidzies 2., 3. un 4. punktā minētais pārskatīšanas periods, izņemot gadījumu, kad izdevēja dalībvalsts ir paziņojusi *CS-SIS* par pagarināšanu, ievērojot 6. punktu. *CS-SIS* četrus mēnešus pirms paredzētās datu dzēšanas par to automātiski informē izdevēju dalībvalsti.

8. Dalībvalstis glabā statistiku par to brīdinājumu par personām skaitu, kuru saglabāšanas periods ir pagarināts saskaņā ar šā panta 6. punktu, un pēc pieprasījuma statistiku nosūta 69. pantā minētajām uzraudzības iestādēm.

9. Tiklīdz *SIRENE* birojam kļūst skaidrs, ka brīdinājums par personu ir sasniedzis savu mērķi un tādēļ tas būtu jādzēš, tas nekavējoties paziņo iestādei, kas izveidojusi brīdinājumu. Iestāde 15 kalendāro dienu laikā no minētā paziņojuma saņemšanas atbild, vai brīdinājums ir dzēsts vai tiks dzēsts, vai norāda iemeslus saglabāt brīdinājumu. Ja atbilde nav saņemta līdz 15 dienu termiņa beigām, *SIRENE* birojs nodrošina, lai brīdinājums tiktu dzēsts. Brīdinājumu dzēš *SIRENE* birojs, ja tas ir pieļaujams saskaņā ar valsts tiesību aktiem. *SIRENE* biroji ziņo savai uzraudzības iestādei, kad, rīkojoties saskaņā ar šo punktu, tie sastopas ar jebkādu problēmu atkārtošanos.

54. pants

Pārskatīšanas periods brīdinājumiem par priekšmetiem

1. Brīdinājumus par priekšmetiem saglabā vienīgi tik ilgi, cik vajadzīgs, lai sasniegtu mērķus, kādiem tie ievadīti.

2. Dalībvalsts 36. un 38. panta nolūkos brīdinājumu par priekšmetiem var ievadīt uz desmit gadiem. Izdevēja dalībvalsts desmit gadu laikā pārskata nepieciešamību saglabāt brīdinājumu.

3. Saskaņā ar 26., 32., 34. un 36. pantu ievadītus brīdinājumus par priekšmetiem pārskata, ievērojot 53. pantu, ja tie ir saistīti ar brīdinājumu par personu. Šādus brīdinājumus saglabā vienīgi tik ilgi, cik ilgi saglabā brīdinājumu par personu.

4. Šā panta 2. un 3. punktā minētajā pārskatīšanas periodā izdevēja dalībvalsts var pieņemt lēmumu brīdinājumu par priekšmetu saglabāt ilgāk par pārskatīšanas periodu, ja izrādās, ka tas ir nepieciešami nolūkos, kādos brīdinājums ievadīts. Šādos gadījumos piemēro attiecīgi 2. vai 3. punktu.

5. Komisija var pieņemt īstenošanas aktus, lai noteiktu īsākus pārskatīšanas periodus konkrētām brīdinājumu par priekšmetiem kategorijām. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

6. Dalībvalstis glabā statistiku par tādu brīdinājumu par priekšmetiem skaitu, kuru saglabāšanas termiņi ir pagarināti saskaņā ar 4. punktu.

XIV NODAĻA
BRĪDINĀJUMU DZĒŠANA

55. pants

Brīdinājumu dzēšana

1. Brīdinājumus par apcietināšanu nolūkā nodot vai izdot, ievērojot 26. pantu, dzēš pēc tam, kad persona ir nodota vai izdota izdevējas dalībvalsts kompetentajām iestādēm. Tos arī dzēš, ja kompetentā tiesu iestāde saskaņā ar valsts tiesību aktiem ir atcēlusi tiesas nolēmumu, uz kura pamata bija izdots brīdinājums. Tos arī dzēš, beidzoties brīdinājuma termiņam saskaņā ar 53. pantu.

2. Brīdinājumus par pazudušām personām vai neaizsargātām personām, kam jāliedz ceļot, ievērojot 32. pantu, dzēš saskaņā ar šādiem noteikumiem:

   a) brīdinājumu par pazudušiem bērniem un nolaupīšanas riskam pakļautiem bērniem dzēš:

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

      ii) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

      iii) saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu;

b) brīdinājumu par pazudušiem pieaugušajiem, ja netiek prasīti nekādi aizsardzības pasākumi, dzēš:

   i) izpildot veicamo darbību, ja izpildītāja dalībvalsts ir konstatējusi viņu atrašanās vietu;

   ii) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

   iii) saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu;

c) brīdinājumu par pazudušiem pieaugušajiem, ja tiek prasīti aizsardzības pasākumi, dzēš:

   i) īstenojot veicamo darbību, ja personai ir piešķirta aizsardzība;

   ii) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

   iii) saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu;

d) brīdinājumu par neaizsargātām personām, kas ir pilngadīgas un kam jāliedz ceļot viņu pašu aizsardzības dēļ, un par bērniem, kam jāliedz ceļot, dzēš:

   i) īstenojot veicamo darbību, piemēram, piešķirot personai aizsardzību;

   ii) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

   iii) saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu.

Neskarot valsts tiesību aktus, ja persona ir ievietota iestādē saskaņā ar kompetentās iestādes lēmumu, brīdinājumu var saglabāt līdz brīdim, kamēr minētā persona ir repatriēta.

3. Brīdinājumus par personām, kuras meklē tiesas procesam, ievērojot 34. pantu, dzēš:

a) personas atrašanās vietu paziņojot izdevējas dalībvalsts kompetentajai iestādei;

b) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

c) saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu.

Ja attiecībā uz informāciju a) apakšpunktā minētajā paziņojumā nevar veikt nekādu rīcību, izdevējas dalībvalsts *SIRENE* birojs par to informē izpildītājas dalībvalsts *SIRENE* biroju nolūkā atrisināt problēmu.

Gadījumā, kad ir konstatēta informācijas atbilsme, ja ziņas par adresi ir nosūtītas izdevējai dalībvalstij, un ja tajā pašā izpildītājā dalībvalstī pēc tam ir konstatēta informācijas atbilsme, kurā tiek konstatēta tā pati adrese, šo informācijas atbilsmi reģistrē izpildītājā dalībvalstī, taču izdevējai dalībvalstij netiek atkārtoti nosūtītas ne ziņas par adresi, ne papildinformācija. Šādos gadījumos izpildītāja dalībvalsts informē izdevēju dalībvalsti par atkārtoto informācijas atbilsmi, un izdevēja dalībvalsts veic visaptverošu, individuālu novērtējumu par nepieciešamību saglabāt brīdinājumu.

4. Brīdinājumus par diskrētu, izmeklēšanas un īpašu pārbaudi, ievērojot 36. pantu, dzēš:

   a) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

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

5. Brīdinājumus par priekšmetiem izņemšanai vai izmantošanai par pierādījumu kriminālprocesā, ievērojot 38. pantu, dzēš:

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

   b) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

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

6. Brīdinājumus par nezināmām meklētām personām, ievērojot 40. pantu, dzēš:

   a) identificējot personu;

   b) beidzoties brīdinājuma termiņam saskaņā ar 53. pantu; vai

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

7. Saskaņā ar 26., 32., 34. un 36. pantu ievadītu brīdinājumu par priekšmetu, ja tas ir saistīts ar brīdinājumu par personu, dzēš, kad saskaņā ar šā pantu tiek dzēsts brīdinājums par personu.

XV NODAĻA
VISPĀRĪGI DATU APSTRĀDES NOTEIKUMI

56. pants

SIS *datu apstrāde*

1. Dalībvalstis apstrādā 20. pantā minētos datus tikai nolūkos, kas noteikti katrai brīdinājumu kategorijai, kas minēta 26., 32., 34., 36., 38. un 40. pantā.

2. Datus kopē vienīgi tehniskos nolūkos, ja šāda kopēšana ir vajadzīga, lai 44. pantā minētās kompetentās iestādes varētu veikt tiešu meklēšanu. Minētajām kopijām piemēro šo regulu. 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 uz laiku, kas nav ilgāks par 48 stundām.

   Dalībvalstis uztur aktuālu minēto kopiju uzskaitījumu, to dara pieejamu uzraudzības iestādēm un nodrošina, lai attiecībā uz minētajām kopijām piemērotu šo regulu, jo īpaši 10. pantu.

4. Šīs regulas 44. pantā minēto valsts kompetento iestāžu piekļuvi *SIS* datiem atļauj vienīgi to kompetences robežās un vienīgi pienācīgi pilnvarotiem darbiniekiem.

5. Attiecībā uz šīs regulas 26., 32., 34., 36., 38. un 40. pantā noteiktajiem brīdinājumiem ikvienai *SIS* informācijas apstrādei citos nolūkos nekā tie, kādēļ tā ievadīta *SIS*, jābūt saistītai ar konkrētu gadījumu un pamatotai ar vajadzību novērst tūlītēju un nopietnu sabiedriskās kārtības un drošības apdraudējumu, ar svarīgiem valsts drošības apsvērumiem vai ar vajadzību novērst smagu noziegumu. Šim nolūkam saņem izdevējas dalībvalsts iepriekšēju atļauju.

6. *SIS* datu izmantošanu, kura neatbilst šā panta 1. līdz 5. punktam, uzskata par ļaunprātīgu izmantošanu saskaņā ar katras dalībvalsts tiesību aktiem, un uz to attiecas sankcijas saskaņā ar 73. pantu.

7. Katra dalībvalsts nosūta *eu-LISA* to savu kompetento iestāžu sarakstu, kuras, ievērojot šo regulu, ir pilnvarotas tieši veikt meklēšanu *SIS* datos, kā arī jebkuras izmaiņas šajā sarakstā. Minētajā sarakstā attiecībā uz katru iestādi norāda, kuros datos un kādos nolūkos tās drīkst veikt meklēšanu. *eu-LISA* nodrošina to, ka saraksts katru gadu tiek publicēts *Eiropas Savienības Oficiālajā Vēstnesī*. *eu-LISA* savā tīmekļa vietnē uztur pastāvīgi atjauninātu sarakstu, kurā ir iekļautas izmaiņas, ko dalībvalstis nosūtījušas starp gadskārtējām publikācijām.

8. Ja vien Savienības tiesību aktos nav paredzēti īpaši noteikumi, attiecīgās valsts *N.SIS* datiem piemēro attiecīgās dalībvalsts tiesību aktus.

57. pants

SIS *dati un valsts datnes*

1. Šīs regulas 56. panta 2. punkts neskar dalībvalsts tiesības savās datnēs glabāt *SIS* datus, saistībā ar kuriem tās teritorijā ir veikta darbība. Tādus datus valsts datnēs saglabā ne ilgāk kā trīs gadus, izņemot gadījumus, kad attiecīgās valsts tiesību aktu īpašos noteikumos ir paredzēts ilgāks saglabāšanas periods.

2. Šīs regulas 56. panta 2. punkts neskar dalībvalsts tiesības savās datnēs saglabāt datus, kas ietverti konkrētā brīdinājumā, ko minētā dalībvalsts ir ievadījusi *SIS*.

58. pants

Informācija brīdinājuma neizpildes gadījumā

Ja pieprasīto darbību nevar veikt, dalībvalsts, no kuras tiek prasīta rīcība, nekavējoties informē izdevēju dalībvalsti papildinformācijas apmaiņas ceļā.

59. pants

SIS *datu kvalitāte*

1. Izdevēja dalībvalsts ir atbildīga par to, lai dati būtu precīzi, atjaunināti un likumīgi ievadīti un uzglabāti *SIS*.

2. Ja izdevēja dalībvalsts saņem attiecīgus papildu vai grozītus datus, kas minēti 20. panta 3. punktā, tā bez kavēšanās pilnīgo vai groza attiecīgo brīdinājumu.

3. Vienīgi izdevēja dalībvalsts ir tiesīga grozīt, papildināt, labot, atjaunināt vai dzēst datus, ko tā ievadījusi *SIS*.

4. Ja dalībvalstij, kura nav izdevēja dalībvalsts, ir attiecīgi papildu vai grozīti dati, kas uzskaitīti 20. panta 3. punktā, šī dalībvalsts papildinformācijas apmaiņas ceļā tos bez kavēšanās nosūta izdevējai dalībvalstij, lai tā varētu pilnīgot vai grozīt brīdinājumu. Ja papildu vai grozītie dati attiecas uz personām, tos nosūta tikai tad, ja ir noskaidrota personas identitāte.

5. Ja dalībvalstij, kura nav izdevēja dalībvalsts, ir pierādījumi, ka datos ir faktu kļūda vai ka dati saglabāti nelikumīgi, tad attiecīgā valsts cik ātri vien iespējams, bet ne vēlāk kā divās darbdienās pēc tam, kad tai kļuvis zināms minētais pierādījums, papildinformācijas apmaiņas ceļā par to informē izdevēju dalībvalsti. Izdevēja dalībvalsts pārbauda šo informāciju un vajadzības gadījumā attiecīgo ierakstu bez kavēšanās labo vai dzēš.

6. Ja dalībvalstis nespēj vienoties divu mēnešu laikā no brīža, kad pirmoreiz atklājās pierādījumi, kas minēti šā panta 5. punktā, tad dalībvalsts, kura nav ievadījusi brīdinājumu, jautājumu nodod attiecīgajām uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītājam lēmuma pieņemšanai, izmantojot sadarbību saskaņā ar 71. pantu.

7. Dalībvalstis apmainās ar papildinformāciju gadījumos, ja persona sūdzas, ka viņa nav tā persona, uz kuru attiecas brīdinājums. Ja pārbaudē konstatē, ka persona, uz kuru attiecas brīdinājums nav sūdzības iesniedzējs, tad sūdzības iesniedzēju informē par 62. pantā minētajiem pasākumiem un tiesībām uz tiesiskās aizsardzības līdzekļiem saskaņā ar 68. panta 1. punktu.

60. pants

Drošības incidenti

1. Jebkurš notikums, kurš ietekmē vai var ietekmēt *SIS* drošību vai var kaitēt *SIS* datiem vai papildinformācijai vai izraisīt to zudumu, ir uzskatāms par drošības incidentu, jo īpaši, ja var būt notikusi nelikumīga piekļuve datiem vai ir bijusi apdraudēta vai var būt bijusi apdraudēta datu pieejamība, integritāte un konfidencialitāte.

2. Drošības incidentus pārvalda tādā veidā, lai nodrošinātu ātru, efektīvu un pareizu reakciju.

3. Neskarot paziņošanu un informēšanu par personas datu aizsardzības pārkāpumu, ievērojot Regulas (ES) 2016/679 33. pantu vai Direktīvas (ES) 2016/680 30. pantu, dalībvalstis, Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra bez kavēšanās paziņo Komisijai, *eu-LISA*, kompetentajai uzraudzības iestādei un Eiropas Datu aizsardzības uzraudzītājam par drošības incidentiem. *eu-LISA* bez kavēšanās paziņo Komisijai un Eiropas Datu aizsardzības uzraudzītājam par jebkādu drošības incidentu saistībā ar centrālo *SIS*.

4. Visām dalībvalstīm bez kavēšanās sniedz informāciju par drošības incidentu, kas ietekmē vai var ietekmēt *SIS* darbību dalībvalstī vai *eu-LISA* vai par citu dalībvalstu ievadīto vai nosūtīto datu vai tās papildinformācijas pieejamību, integritāti un konfidencialitāti, ar kuru notikusi apmaiņa, un par to ziņo saskaņā ar incidentu pārvaldības plānu, ko nodrošina *eu-LISA*.

5. Drošības incidenta gadījumā dalībvalstis un *eu-LISA* sadarbojas.

6. Komisija par nopietniem incidentiem nekavējoties ziņo Eiropas Parlamentam un Padomei. Minētos ziņojumus klasificē kā *EU RESTRICTED/RESTREINT UE* saskaņā ar piemērojamiem drošības noteikumiem.

7. Ja drošības incidenta iemesls ir datu ļaunprātīga izmantošana, dalībvalstis, Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra nodrošina, lai saskaņā ar 73. pantu tiktu piemērotas sankcijas.

61. pants

Personu ar līdzīgām īpašībām atšķiršana

1. Ja, ievadot jaunu brīdinājumu, konstatē, ka *SIS* jau ir brīdinājums par personu ar tādu pašu identitātes aprakstu, *SIRENE* birojs 12 stundu laikā papildinformācijas apmaiņas ceļā sazinās ar izdevēju dalībvalsti, lai šķērspārbaudē noskaidrotu, vai abu brīdinājumu subjekts ir viena un tā pati persona.

2. Ja šķērspārbaudē atklājas, ka jaunā brīdinājuma subjekts un persona, uz kuru attiecas brīdinājums, kas jau ievadīts *SIS*, patiešām ir viena un tā pati persona, *SIRENE* birojs piemēro 23. pantā minēto procedūru vairāku brīdinājumu ievadīšanai.

3. Ja šķērspārbaudē atklājas, ka tās ir divas dažādas personas, *SIRENE* birojs apstiprina lūgumu ievadīt otru brīdinājumu, pievienojot datus, kas vajadzīgi, lai novērstu nepareizu identifikāciju.

62. pants

Papildu dati, ko izmanto attiecībā uz ļaunprātīgi izmantotu identitāti

1. Ja personu, uz kuru attiecas brīdinājums, var sajaukt ar personu, kuras identitāte ir izmantota ļaunprātīgi, izdevēja dalībvalsts ar tās personas skaidri izteiktu piekrišanu, kuras identitāte ir ļaunprātīgi izmantota, brīdinājumam pievieno datus par pēdējo minēto personu, lai izvairītos no nepareizas identifikācijas negatīvām sekām. Ikvienai personai, kuras identitāte ir ļaunprātīgi izmantota, ir tiesības atsaukt savu piekrišanu attiecībā uz pievienoto personas datu apstrādi.

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 attiecas brīdinājums; un

   b) lai personai, kuras identitāte ir izmantota ļaunprātīgi, ļautu pierādīt savu īsto identitāti un konstatēt, ka tās identitāte ir izmantota ļaunprātīgi.

3. Šā panta nolūkiem un saskaņā ar personas, kuras identitāte ir ļaunprātīgi izmantota, nepārprotamu piekrišanu attiecībā uz katru datu kategoriju, *SIS* attiecībā uz personu, kuras identitāte ir izmantota ļaunprātīgi, drīkst ievadīt un turpmāk apstrādāt vienīgi šādus personas datus:

   a) uzvārdi;

   b) vārdi;

c) vārdi, uzvārdi dzimšanas brīdī;

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

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

f) dzimšanas vieta;

g) dzimšanas datums;

h) dzimums;

i) fotogrāfijas un sejas attēli;

j) pirkstu nospiedumi, plaukstu nospiedumi vai abi;

k) visas valstspiederības;

l) personas identifikācijas dokumentu kategorija;

m) personas identifikācijas dokumentu izdošanas valsts;

n) personas identifikācijas dokumentu numurs(-i);

o) personas identifikācijas dokumentu izdošanas datums;

p) personas adrese;

q) personas tēva vārds, uzvārds;

r) personas mātes vārds, uzvārds.

4. Komisija pieņem īstenošanas aktus, lai noteiktu un pilnveidotu tehniskos noteikumus, kas vajadzīgi šā panta 3. punktā minēto datu ievadīšanai un turpmākai apstrādei. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

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

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

63. 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 pārskatīšanas 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 operatīva vajadzība.

5. Ja dalībvalsts uzskata, ka citas dalībvalsts veikta brīdinājumu sasaiste ir pretrunā tās tiesību aktiem vai tās 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. Komisija pieņem īstenošanas aktus, lai noteiktu un izstrādātu tehniskos noteikumus par brīdinājumu sasaisti. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

64. 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 minētās dalībvalsts ievadītu brīdinājumu vai uz brīdinājumu, saistībā ar kuru tās teritorijā ir veikta darbība. Termiņu, cik ilgi atļauts minētajās datnēs glabāt šādus datus, reglamentē attiecīgās valsts tiesību akti.

65. pants

Personas datu nodošana trešām personām

SIS apstrādātos datus un ar tiem saistīto papildinformāciju, ar kuriem, ievērojot šo regulu, ir notikusi apmaiņa, nenodod un nedara pieejamus trešām valstīm vai starptautiskām organizācijām.

XVI NODAĻA
DATU AIZSARDZĪBA

66. pants

Piemērojamie tiesību akti

1. Regulu (ES) 2018/…[+] piemēro personas datu apstrādei, ko saskaņā ar šo regulu veic *eu-LISA*, Eiropas Robežu un krasta apsardzes aģentūra un *Eurojust*. Regulu (ES) 2016/794 piemēro personas datu apstrādei, ko veic Eiropols saskaņā ar šo regulu.

2. Direktīvu (ES) 2016/680 piemēro personas datu apstrādei, ko saskaņā ar šo regulu veic valsts kompetentās iestādes un dienesti, lai novērstu, atklātu, izmeklētu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināLsodus, tostarp, lai aizsargātu pret sabiedriskās drošības apdraudējumiem un novērstu tos.

[+] OV: lūgums ievietot dokumentā PE-CONS 31/18 ietvertās regulas numuru.

3. Regulu (ES) 2016/679 piemēro tādai personas datu apstrādei, ko saskaņā ar šo regulu veic valsts kompetentās iestādes un dienesti, izņemot apstrādi, ko veic, lai novērstu, atklātu, izmeklētu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināls odus, tostarp, lai aizsargātu pret sabiedriskās drošības apdraudējumiem un novērstu tos.

67. pants

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

1. Datu subjekti var īstenot tiesības, kas noteiktas Regulas (ES) Nr. 2016/679 15., 16. un 17. pantā un Direktīvas (ES) 2016/680 14. pantā un 16. panta 1. un 2. punktā.

2. Dalībvalsts, kas nav izdevēja dalībvalsts, datu subjektam informāciju par visiem datu subjekta personas datiem, kas tiek apstrādāti, var sniegt vienīgi tad, ja tā iepriekš ir devusi iespēju izdevējai dalībvalstij darīt zināmu savu nostāju. Saziņa starp minētajām dalībvalstīm notiek papildinformācijas apmaiņas ceļā.

3. 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 pasākums demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgā datu subjekta pamattiesības un leģitīmās intereses, lai:

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

b) novērstu, ka tiek traucēta noziedzīgu nodarījumu novēršana, atklāšana un izmeklēšana vai saukšana pie atbildības par tiem, vai kriminālsodu izpilde;

c) aizsargātu sabiedrisko drošību;

d) aizsargātu valsts drošību; vai

e) aizsargātu citu personu tiesības un brīvības.

Pirmajā daļā minētajos gadījumos dalībvalsts bez liekas kavēšanās rakstiski informē datu subjektu par jebkādu piekļuves atteikumu vai ierobežojumu un par atteikuma vai ierobežojuma iemesliem. Šādu informāciju var nesniegt, ja tās sniegšana apdraudētu jebkādu no pirmās daļas a) - e) apakšpunktā noteiktajiem nolūkiem. Dalībvalsts informē datu subjektu par iespēju iesniegt sūdzību uzraudzības iestādē vai vērsties tiesā.

Dalībvalsts dokumentē faktiskos vai juridiskos iemeslus, kuri ir pamatā lēmumam nesniegt datu subjektam informāciju. Minēto informāciju dara pieejamu uzraudzības iestādēm.

Šādos gadījumos datu subjekts var īstenot savas tiesības arī ar kompetento uzraudzības iestāžu starpniecību.

4. Pēc pieteikuma attiecībā uz piekļuvi datiem, to labošanu vai dzēšanu dalībvalsts datu subjektu, cik drīz vien iespējams un jebkurā gadījumā Regulas (ES) 2016/679 12. panta 3. punktā noteiktajos termiņos, informē par pēcpasākumiem, kas veikti, lai īstenotu tiesības saskaņā ar šo pantu.

68. pants

Tiesiskās aizsardzības līdzekļi

1. Neskarot Regulas (ES) Nr. 2016/679 un Direktīvas (ES) 2016/680 noteikumus par tiesiskās aizsardzības līdzekļiem, ikviena persona var vērsties jebkurā kompetentajā iestādē, tostarp tiesā, saskaņā ar jebkuras dalībvalsts tiesību aktiem, lai piekļūtu informācijai, to labotu, dzēstu un iegūtu vai lai saņemtu kompensāciju saistībā ar brīdinājumu, kas attiecas uz personu.

2. Neskarot 72. pantu, dalībvalstis savstarpēji apņemas pildīt galīgos lēmumus, ko pieņem tiesa vai šā panta 1. punktā minētās iestādes.

3. Dalībvalstis katru gadu Eiropas Datu aizsardzības kolēģijai ziņo par:

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

   b) piekļuves pieprasījumu skaitu, kas iesniegti 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 uzraudzības iestādei par neprecīzu datu labošanu un nelikumīgi glabātu datu dzēšanu;

e) uzsākto tiesas procesu skaitu;

f) to gadījumu skaitu, kad tiesa lēmusi par labu prasītājam;

g) visiem novērojumiem gadījumos, kad ir savstarpēji atzīti citu dalībvalstu tiesu vai iestāžu pieņemti galīgie lēmumi attiecībā uz brīdinājumiem, kurus ievadījusi izdevēja dalībvalsts.

Komisija izstrādā šajā punktā minētās ziņošanas veidni.

4. Dalībvalstu ziņojumus iekļauj 71. panta 4. punktā minētajā kopīgajā pārskatā.

69. pants

N.SIS *uzraudzība*

1. Dalībvalstis nodrošina, lai neatkarīgas uzraudzības iestādes, kas norīkotas katrā dalībvalstī un kam piešķirtas Regulas (ES) 2016/679 VI nodaļā vai Direktīvas (ES) 2016/680 VI nodaļā vai minētās pilnvaras, uzraudzītu personas datu *SIS* apstrādes likumību attiecīgās valsts teritorijā, to nosūtīšanas likumību no attiecīgās valsts teritorijas, un papildinformācijas apmaiņas un turpmākās apstrādes likumību tās teritorijā.

2. Attiecīgās uzraudzības iestādes nodrošina, lai vismaz reizi četros gados tiltu veikta attiecīgās valsts *N.SIS* veikto datu apstrādes operāciju revīzija saskaņā ar starptautiskiem revīzijas standartiem. Revīziju veic uzraudzības iestādes, vai uzraudzības iestādes tieši pasūta revīziju, ko veic neatkarīgs datu aizsardzības revidents. Uzraudzības iestādes vienmēr saglabā kontroli pār neatkarīgo revidentu un uzņemas atbildību.

3. Dalībvalstis nodrošina, lai to uzraudzības iestādēm būtu pietiekami resursi ar šo regulu tām uzticēto uzdevumu izpildei, un piekļuve tādu personu sniegtām konsultācijām, kurām ir pietiekamas zināšanas par biometriskajiem datiem.

70. pants

eu-LISA *uzraudzība*

1. Eiropas Datu aizsardzības uzraudzītājs ir atbildīgs par *eu-LISA* veiktās personas datu apstrādes uzraudzību, kā arī par to, lai tiktu nodrošināta tās veikšana saskaņā ar šo regulu. Attiecīgi piemēro uzdevumus un pilnvaras, kas minēti Regulas (ES) 2018/...[+] 57. un 58. pantā.

2. Eiropas Datu aizsardzības uzraudzītājs vismaz reizi četros gados veic *eu-LISA* veiktās personas datu apstrādes revīziju saskaņā ar starptautiskiem revīzijas standartiem. Ziņojumu par minēto revīziju nosūta Eiropas Parlamentam, Padomei, *eu-LISA*, Komisijai un uzraudzības iestādēm. Pirms ziņojuma pieņemšanas *eu-LISA* dod iespēju izteikt savus apsvērumus.

[+] OV: lūgums ievietot dokumentā PE-CONS 31/18 ietvertās regulas numuru.

71. pants

Uzraudzības iestāžu

un Eiropas Datu aizsardzības uzraudzītāja sadarbība

1. 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, uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs apmainās ar attiecīgu 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 uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs tiekas vismaz divreiz gadā Eiropas Datu aizsardzības kolēģijas ietvaros. Šo sanāksmju izmaksas sedz un rīkošanu uzņemas Eiropas Datu aizsardzības kolēģija. Pirmajā sanāksmē pieņem reglamentu. Ja nepieciešams, kopīgi izstrādā turpmākas darba metodes.

4. Kopīgu darbības pārskatu par koordinēto uzraudzību Eiropas Datu aizsardzības kolēģija katru gadu nosūta Eiropas Parlamentam, Padomei un Komisijai.

XVII NODAĻA
ATBILDĪBA UN SANKCIJAS

72. pants

Atbildība

1. Neskarot tiesības uz kompensāciju un jebkādu atbildību saskaņā ar Regulu (ES) 2016/679, Direktīvu (ES) 2016/680 un Regulu (ES) 2018/…[+]:

   a) jebkurai personai vai dalībvalstij, kam nodarīts materiāls vai nemateriāls kaitējums tādas nelikumīgas personas datu apstrādes darbības rezultātā, kura veikta, izmantojot *N.SIS*, vai jebkuras citas ar šo regulu nesaderīgas rīcības rezultātā, kuru veikusi dalībvalsts, ir tiesības saņemt kompensāciju no minētās dalībvalsts; un

   b) jebkurai personai vai dalībvalstij, kam nodarīts materiāls vai nemateriāls kaitējums jebkuras ar šo regulu nesaderīgas *eu-LISA* rīcības rezultātā, ir tiesības saņemt kompensāciju no *eu-LISA*.

   Dalībvalsti vai *eu-LISA* pilnībā vai daļēji atbrīvo no to atbildības saskaņā ar pirmo daļu, ja tās pierāda, ka nav atbildīgas par notikumu, kas izraisījis minēto kaitējumu.

[+] OV: lūgums ievietot dokumentā PE-CONS 31/18 ietvertās regulas numuru.

2. Ja saistībā ar to, ka kāda dalībvalsts nav ievērojusi pienākumus saskaņā ar šo regulu, ir nodarīts kaitējums *SIS*, minētā dalībvalsts ir atbildīga par šādu kaitējumu, izņemot gadījumu, kad un ciktāl *eu-LISA* vai cita dalībvalsts, kas piedalās *SIS*, nav veikusi saprātīgus pasākumus, lai kaitējumu novērstu vai mazinātu tā sekas.

3. Pret dalībvalsti vērstas kompensācijas prasības par kaitējumu, kā minēts 1. un 2. punktā, reglamentē minētās dalībvalsts tiesību akti. Pret *eu-LISA* vērstām kompensācijas prasībām par kaitējumu, kā minēts 1. un 2. punktā, piemēro Līgumos paredzētos nosacījumus.

73. pants

Sankcijas

Dalībvalstis nodrošina, lai jebkāda *SIS* datu ļaunprātīga izmantošana vai šādu datu apstrāde, vai jebkāda papildinformācijas apmaiņa, kas ir pretrunā šai regulai, būtu sodāma saskaņā ar valsts tiesību aktiem.

Paredzētās sankcijas ir iedarbīgas, samērīgas un atturošas.

XVIII NODAĻA
NOBEIGUMA NOTEIKUMI

74. pants

Uzraudzība un statistika

1. *eu-LISA* 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, ziņošanas par datu kvalitāti un statistikas nolūkos *eu-LISA* ir piekļuve vajadzīgajai informācijai, kas attiecas uz apstrādes darbībām, kuras veic centrālajā *SIS*.

3. *eu-LISA* sagatavo dienas, mēneša un gada statistiku, norādot ierakstu skaitu pa brīdinājumu kategorijām, gan par katru dalībvalsti, gan kopumā. *eu-LISA* sniedz arī ikgadējus ziņojumus par saņemto informācijas atbilsmju skaitu pa brīdinājumu kategorijām, to, cik reizes notikusi meklēšana *SIS*, un to, cik reizes piekļūts *SIS*, lai ievadītu, atjauninātu vai dzēstu brīdinājumu, gan par katru dalībvalsti, gan kopumā. Apkopotajā statistikā neiekļauj personas datus. Gada statistikas ziņojumu publicē.

4. Dalībvalstis, Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra sniedz *eu-LISA* un Komisijai informāciju, kas nepieciešama, lai izstrādātu 3., 6., 8. un 9. punktā minētos ziņojumus.

5. Šajā informācijā ir ietverti atsevišķi statistikas dati par to, cik reižu meklēšanu ir veikuši tādi dalībvalstu dienesti vai meklēšana ir veikta tādu dalībvalstu dienestu vārdā, kuri 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; un gaisa kuģiem, tostarp gaisa kuģu dzinējiem; un šaujamieročiem. Statistikā uzrāda arī informācijas atbilsmju skaitu pa brīdinājumu kategorijām.

6. *eu-LISA* iesniedz Eiropas Parlamentam, Padomei, dalībvalstīm, Komisijai, Eiropolam, *Eurojust*, Eiropas Robežu un krasta apsardzes aģentūrai un Eiropas Datu aizsardzības uzraudzītājam visus sagatavotos statistikas ziņojumus.

Lai uzraudzītu to, kā tiek īstenoti Savienības tiesību akti, tostarp Regulas (ES) Nr. 1053/2013 nolūkos, Komisijai var pieprasīt, lai *eu-LISA* regulāri vai *ad hoc* kārtā sniegtu papildu īpašus statistikas ziņojumus par *SIS* darbību, *SIS* izmantošanu un par papildinformācijas apmaiņu.

Eiropas Robežu un krasta apsardzes aģentūra var *eu-LISA* prasīt regulāri vai *ad hoc* kārtā sniegt papildu īpašus statistikas ziņojumus Regulas (ES) 2016/1624 11. un 13. pantā minētās riska analīzes un neaizsargātības novērtējumu veikšanas nolūkā.

7. Šīs regulas 15. panta 4. punkta un šā panta 3., 4. un 6. punkta nolūkos *eu-LISA* izveido, īsteno un mitina savos tehniskajos centros centrālo repozitoriju, kurš satur datus, kas minēti 15. panta 4. punktā un šā panta 3. punktā, un kurš neļauj identificēt personas un ļauj Komisijai un šā panta 6. punktā minētajām aģentūrām iegūt minētos ziņojumus un statistiku. Pēc pieprasījuma *eu-LISA* dalībvalstīm un Komisijai, kā arī Eiropolam, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūrai, ciktāl tas ir nepieciešams viņu pienākumu pildīšanai, sniedz piekļuvi centrālajam repozitorijam ar aizsargātu piekļuvi, izmantojot komunikācijas infrastruktūru. *eu-LISA* veic piekļuves kontroles un konkrētus lietotāju profilus, lai nodrošinātu, ka centrālajam repozitorijam piekļūst vienīgi ziņojumu un statistikas nolūkā.

8. Divus gadus pēc šīs regulas piemērošanas dienas, ievērojot 79. panta 5. punkta pirmo daļu, un pēc tam reizi divos gados *eu-LISA* iesniedz Eiropas Parlamentam un Padomei ziņojumu par centrālās *SIS* un komunikācijas infrastruktūras tehnisko darbību, tostarp to drošību, par *AFIS* un par divpusējo un daudzpusējo papildinformācijas apmaiņu starp dalībvalstīm. Tiklīdz tehnoloģija tiek izmantota, šajā ziņojumā ietver arī izvērtējumu par sejas attēlu izmantošanu personu identifikācijai.

9. Trīs gadus pēc šīs regulas piemērošanas dienas, ievērojot 79. panta 5. punkta pirmo daļu, un pēc tam reizi četros gados Komisija veic vispārēju izvērtēšanu par centrālo *SIS* un divpusējo un daudzpusējo papildinformācijas apmaiņu starp dalībvalstīm. Minētajā vispārējā izvērtējumā 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. Šajā izvērtējuma ziņojumā iekļauj arī novērtējumu par *AFIS* un *SIS* informācijas kampaņām, ko Komisija veikusi saskaņā ar 19. pantu.

Komisija izvērtējuma ziņojumu nosūta Eiropas Parlamentam un Padomei.

10. Komisija pieņem īstenošanas aktus, lai noteiktu sīki izstrādātus noteikumus par šā panta 7. punktā minētā centrālā repozitorija darbību un datu aizsardzības un drošības noteikumus, ko piemēro minētajam repozitorijam. Minētos īstenošanas aktus pieņem saskaņā ar 76. panta 2. punktā minēto pārbaudes procedūru.

75. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 38. panta 3. punktā un 43. panta 4. punktā minētos deleģētos aktus Komisijai piešķir uz nenoteiktu laiku no ... [šīs regulas spēkā stāšanās diena].

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 38. panta 3. punktā un 43. panta 4. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.

4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar ekspertiem, kurus katra dalībvalsts iecēlusi saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.

5. Tiklīdz Komisija pieņem deleģētu aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

6. Saskaņā ar 38. panta 3. punktu vai 43. panta 4. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus, vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

76. pants

Komiteju procedūra

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

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

77. pants

Grozījumi Lēmumā 2007/533/TI

Lēmumu 2007/533/TI groza šādi:

1) lēmuma 6. pantu aizstāj ar šādu:

"*6. pants*

Valstu sistēmas

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

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

2) lēmuma 11. pantu aizstāj ar šādu:

"*11. pants*
Konfidencialitāte – dalībvalstis

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

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

3. *N.SIS II* vai jebkādas tehnisko kopiju darbības pārvaldība netiek uzticēta privātiem uzņēmumiem vai privātām organizācijām.";

3) lēmuma 15. pantu groza šādi:

a) iekļauj šādu punktu:

"3.a Pārvaldības iestāde izstrādā un uztur mehānismu un procedūras *CS-SIS* datu kvalitātes pārbaužu veikšanai. Šajā sakarā tā regulāri iesniedz ziņojumus dalībvalstīm.

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

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

b) panta 8. punktu aizstāj ar šādu:

"8. Centrālās *SIS II* darbības pārvaldība ir visi uzdevumi, kas vajadzīgi, lai saskaņā ar šo lēmumu nodrošinātu centrālās *SIS II* darbību 24 stundas diennaktī 7 dienas nedēļā, jo īpaši uzturēšanas darbi un tehniski pielāgojumi, kas vajadzīgi sistēmas nevainojamai darbībai. Minētie uzdevumi ietver arī centrālās *SIS II* un *N.SIS II* testēšanas pasākumu koordinēšanu, vadību un atbalstīšanu, kas nodrošina, ka centrālā *SIS II* un *N.SIS II* darbojas saskaņā ar tehniskās atbilstības prasībām, kuras izklāstītas 9. pantā.";

4) lēmuma 17. pantā pievieno šādus punktus:

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

4. *CS-SIS* darbības pārvaldība netiek uzticēta privātiem uzņēmumiem vai privātām organizācijām.";

5) lēmuma 21. pantam pievieno šādu daļu:

"Ja personu vai priekšmetu meklē saistībā ar brīdinājumu par teroristu nodarījumu, konkrēto gadījumu uzskata par atbilstīgu, piemērotu un pietiekami svarīgu, lai būtu brīdinājums *SIS II*. Sabiedriskās vai valsts drošības apsvērumu dēļ dalībvalstis var izņēmuma kārtā atturēties ievadīt brīdinājumu, ja tas varētu traucēt oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras.";

6) lēmuma 22. pantu aizstāj ar šādu:

"*22. pants*
Īpaši noteikumi ievadīšanai, pārbaudei vai meklēšanai, izmantojot fotogrāfijas un pirkstu nospiedumus

1. Fotogrāfijas un pirkstu nospiedumus ievada tikai pēc īpašas kvalitātes pārbaudes, lai apstiprinātu, ka tie atbilst minimālajiem datu kvalitātes standartiem. Īpašās kvalitātes pārbaudes specifikāciju nosaka saskaņā ar 67. pantā minēto procedūru.

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

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

4. Pirkstu nospiedumu datos *SIS II* saistībā ar brīdinājumiem, kuri ievadīti saskaņā ar 26., 32. un 36. pantu, var meklēt arī, izmantojot pilnus vai nepilnus tādu pirkstu nospiedumu komplektus, kuri konstatēti izmeklējamu smagu noziegumu vai teroristu nodarījumu izdarīšanas vietās, ja ar augstu varbūtības pakāpi var konstatēt, ka minētie nospiedumu komplekti pieder nodarījuma izdarītājam, un ar noteikumu, ka meklēšanu veic vienlaikus dalībvalsts attiecīgajās valstu pirkstu nospiedumu datubāzēs.";

7) lēmuma 41. pantu aizstāj ar šādu:

"*41. pants*
Eiropola piekļuve SIS II *datiem*

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

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

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

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

5. Eiropols:

a) neskarot 4. un 6. punktu, nesasaista *SIS II* daļas un nepārsūta tur esošos datus, kuriem tas var piekļūt, nevienai datu vākšanas un apstrādes sistēmai, ko ekspluatē Eiropols vai kas tiek ekspluatēta Eiropolā, kā arī neveic nekādu *SIS II* daļu lejupielādi vai citādu kopēšanu;

b) neatkarīgi no Regulas (ES) 2016/794 31. panta 1. punkta dzēš papildinformāciju, kas satur personas datus, ne vēlāk kā vienu gadu pēc saistītā brīdinājuma dzēšanas. Atkāpjoties no šā noteikuma, ja Eiropolam tā datubāzēs vai operatīvās analīzes projektos ir informācija par gadījumu, ar kuru papildinformācija ir saistīta, lai Eiropols varētu veikt savus uzdevumus, Eiropols, ja vajadzīgs, izņēmuma kārtā var turpināt glabāt papildinformāciju. Eiropols informē izdevēju un izpildītāju dalībvalsti, ka šādu papildinformāciju turpina glabāt, un sniedz tam pamatojumu;

c) tiesības piekļūt *SIS II* datiem, tostarp papildinformācijai, nodrošina vienīgi īpaši pilnvarotiem Eiropola darbiniekiem, kuriem piekļuve šādiem datiem nepieciešama viņu pienākumu pildīšanai;

d) pieņem un piemēro pasākumus ar mērķi nodrošināt drošību, konfidencialitāti un pašuzraudzību saskaņā ar 10., 11. un 13. pantu;

e) nodrošina, ka darbinieki, kam ir tiesības apstrādāt *SIS II* datus, tiek pienācīgi apmācīti un saņem informāciju saskaņā ar 14. pantu; un

f) neskarot Regulu (ES) 2016/794, ļauj Eiropas Datu aizsardzības uzraudzītājam uzraudzīt un pārskatīt Eiropola darbības, ko tas veic, īstenojot tiesības piekļūt *SIS II* datiem un meklēt tajos, un to, kā tas veic papildinformācijas apmaiņu un apstrādi.

6. Eiropols datus no *SIS II* kopē vienīgi tehniskos nolūkos, ja šāda kopēšana ir vajadzīga, lai pienācīgi pilnvaroti Eiropola darbinieki varētu veikt tiešu meklēšanu šajos datos. Uz šādām kopijām attiecas šis lēmums. Tehnisko kopiju izmanto vienīgi tam, lai saglabātu *SIS II* datus, kamēr tajos notiek meklēšana. Tiklīdz meklēšana ir pabeigta, datus dzēš. Šādu izmantošanu neuzskata par *SIS II* datu nelikumīgu lejupielādi vai kopēšanu. Eiropols nekopē brīdinājumu datus vai papildu datus, ko izdevušas dalībvalstis, vai no *CS-SIS II* citās Eiropola sistēmās.

7. Lai pārbaudītu datu apstrādes likumību, veiktu pašuzraudzību un nodrošinātu datu pienācīgu drošību un integritāti, Eiropols saglabā reģistra ierakstus par katru piekļuvi un meklēšanu *SIS II* saskaņā ar 12. panta noteikumiem. Šādus reģistra ierakstus un dokumentus neuzskata par *SIS II* daļu nelikumīgu lejupielādi vai kopēšanu.

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

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

---

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

8) iekļauj šādu pantu:

"*42.a pants*

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

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

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

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

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

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

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

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

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

---

* 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.).

** Eiropas Parlamenta un Padomes Regula (ES) 2018/... (… gada …) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV ...).".

[+] OV: lūgums ievietot tekstā numuru un papildināt zemsvītras piezīmē ietverto publikācijas atsauci dokumentā PE-CONS 31/18 iekļautajai regulai.

78. pants

Atcelšana

Regulu (EK) Nr. 1986/2006 un Lēmumu 2007/533/TI un Lēmumu 2010/261/ES atceļ no šīs regulas piemērošanas dienas kā noteikts 79. panta 5. punkta pirmajā daļā.

Atsauces uz atcelto Regulu (EK) Nr. 1986/2006 un Lēmumu 2007/533/TI uzskata par atsaucēm uz šo regulu, un tās lasa saskaņā ar pielikumā iekļautajām atbilstības tabulām.

79. pants

Stāšanās spēkā, darbības un piemērošanas sākums

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

2. Ne vēlāk kā … [trīs gadi pēc šīs regulas stāšanās spēkā] Komisija pēc tam, kad tā ir pārbaudījusi, vai ir izpildīti turpmāk uzskaitītie nosacījumi, pieņem lēmumu, kurā nosaka dienu, kad *SIS* sāk darbību, ievērojot šo regulu:

   a) ir pieņemti šīs regulas piemērošanai vajadzīgie īstenošanas akti;

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

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

3. Komisija rūpīgi uzrauga 2. punktā izklāstīto pakāpeniskas nosacījumu izpildes procesu un informē Eiropas Parlamentu un Padomi par minētajā punktā minētās pārbaudes iznākumu.

4. Līdz ... [viens gads pēc šīs regulas spēkā stāšanās dienas] un katru gadu pēc tam, kamēr vēl nav pieņemts 2. punktā minētais Komisijas lēmums, Komisija iesniedz ziņojumu Eiropas Parlamentam un Padomei par stāvokli sagatavošanas darbos šīs regulas pilnīgai īstenošanai. Minētajā ziņojumā ir iekļauta arī detalizēta informācija par radītajām izmaksām un informācija par jebkādiem riskiem, kas var ietekmēt kopējās izmaksas.

5. Šo regulu piemēro no dienas, kas noteikta saskaņā ar 2. punktu.

Atkāpjoties no pirmās daļas:

a) regulas 4. panta 4. punktu, 5. pantu, 8. panta 4. punktu, 9. panta 1. un 5. punktu, 12. panta 8. punktu, 15. panta 7. punktu, 19. pantu, 20. panta 4. un 5. punktu, 26. panta 6. punktu, 32. panta 9. punktu, 34. panta 3. punktu, 36. panta 6. punktu, 38. panta 3. un 4. punktu, 42. panta 5. punktu, 43. panta 4. punktu, 54. panta 5. punktu, 62. panta 4. punktu, 63. panta 6. punktu, 74. panta 7. un 10. punktu, 75. un 76. pantu, 77. panta 1) līdz 5) punktu un šā panta 3. un 4. punktu piemēro no šīs regulas spēkā stāšanās dienas;

b) regulas 77. panta 7) un 8) punktu piemēro no … [gads pēc šīs regulas spēkā stāšanās dienas];

c) regulas 77. panta 6) punktu piemēro no… [divi gadi pēc šīs regulas spēkā stāšanās dienas].

6. Šā panta 2. punktā minēto Komisijas lēmumu publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama dalībvalstīs saskaņā ar Līgumiem.

Briselē,

Eiropas Parlamenta vārdā —	*Padomes vārdā —*
priekšsēdētājs	*priekšsēdētājs*

PIELIKUMS

Atbilstības tabulas

Lēmums 2007/533/TI	Šī regula
1. pants	1. pants
2. pants	2. pants
3. pants	3. pants
4. pants	4. pants
5. pants	5. pants
6. pants	6. pants
7. pants	7. pants
8. pants	8. pants
9. pants	9. pants
10. pants	10. pants
11. pants	11. pants
12. pants	12. pants
13. pants	13. pants
14. pants	14. pants
15. pants	15. pants
16. pants	16. pants
17. pants	17. pants
18. pants	18. pants
19. pants	19. pants
20. pants	20. pants
21. pants	21. pants
22. pants	42. un 43. pants

Lēmums 2007/533/TI	Šī regula
23. pants	22. pants
–	23. pants
24. pants	24. pants
25. pants	25. pants
26. pants	26. pants
27. pants	27. pants
28. pants	28. pants
29. pants	29. pants
30. pants	30. pants
31. pants	31. pants
32. pants	32. pants
33. pants	33. pants
34. pants	34. pants
35. pants	35. pants
36. pants	36. pants
37. pants	37. pants
38. pants	38. pants
39. pants	39. pants
–	40. pants
–	41. pants
40. pants	44. pants
–	45. pants
–	46. pants
–	47. pants

Lēmums 2007/533/TI	Šī regula
41. pants	48. pants
42. pants	49. pants
–	51. pants
42.a pants	50. pants
43. pants	52. pants
44. pants	53. pants
45. pants	54. pants
–	55. pants
46. pants	56. pants
47. pants	57. pants
48. pants	58. pants
49. pants	59. pants
–	60. pants
50. pants	61. pants
51. pants	62. pants
52. pants	63. pants
53. pants	64. pants
54. pants	65. pants
55. pants	–
56. pants	–
57. pants	66. pants
58. pants	67. pants
59. pants	68. pants
60. pants	69. pants

Lēmums 2007/533/TI	Šī regula
61. pants	70. pants
62. pants	71. pants
63. pants	–
64. pants	72. pants
65. pants	73. pants
66. pants	74. pants
–	75. pants
67. pants	76. pants
68. pants	–
–	77. pants
69. pants	–
–	78. pants
70. pants	–
71. pants	79. pants

Regula (EK) Nr. 1986/2006	Šī regula
1., 2. un 3. pants	45. pants