Eiropas Savienības

Oficiālais Vēstnesis

L 135

Izdevums latviešu valodā

Tiesību akti

62. gadagājums

2019. gada 22. maijs

Saturs

I

(Leģislatīvi akti)

REGULAS

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2019/816

(2019. gada 17. aprīlis),

ar ko Eiropas Sodāmības reģistru informācijas sistēmas papildināšanai izveido centralizētu sistēmu (*ECRIS-TCN*) tādu dalībvalstu identificēšanai, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un ar ko groza Regulu (ES) 2018/1726

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 82. panta 1. punkta otrās daļas d) apakšpunktu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

saskaņā ar parasto likumdošanas procedūru ([1]),

tā kā:

(1) Savienība ir noteikusi sev mērķi – piedāvāt saviem pilsoņiem brīvības, drošības un tiesiskuma telpu bez iekšējām robežām, kurā ir nodrošināta personu brīva pārvietošanās. Minētais mērķis būtu jāsasniedz, cita starpā izmantojot piemērotus pasākumus, lai novērstu un apkarotu noziedzību, tostarp organizēto noziedzību un terorismu.

(2) Šis mērķis paredz, ka informācija par notiesājošiem spriedumiem, kas pasludināti dalībvalstīs, ir jāņem vērā ārpus notiesāšanas dalībvalsts jauna kriminālprocesa gaitā, kā noteikts Padomes Pamatlēmumā 2008/675/TI ([2]), kā arī nolūkā novērst jaunus noziedzīgus nodarījumus.

(3) Minētais mērķis paredz tādas informācijas apmaiņu starp dalībvalstu kompetentajām iestādēm, kura iegūta no sodāmības reģistriem. Šādu informācijas apmaiņu organizē un veicina noteikumi, kas izklāstīti Padomes Pamatlēmumā 2009/315/TI ([3]), un Eiropas Sodāmības reģistru informācijas sistēmā (*ECRIS*), kas izveidota saskaņā ar Padomes Lēmumu 2009/316/TI ([4]).

(4) Tomēr esošais *ECRIS* tiesiskais regulējums nepievēršas pietiekamā mērā to lūgumu aspektiem, kuri attiecas uz trešo valstu valstspiederīgajiem. Lai gan, izmantojot *ECRIS*, jau ir iespējams apmainīties ar informāciju par trešo valstu valstspiederīgajiem, nav vienotas Savienības procedūras vai mehānisma, lai to darītu efektīvi, ātri un precīzi.

(5) Informācija par trešo valstu valstspiederīgajiem Savienībā netiek vākta valstspiederības dalībvalstī, kā tas notiek attiecībā uz dalībvalstu valstspiederīgajiem, bet tiek tikai uzglabāta tajās dalībvalstīs, kurās ir pasludināti notiesājošie spriedumi. Tāpēc pilnīgu pārskatu par kāda trešās valsts valstspiederīgā sodāmības vēsturi var nodrošināt tikai tad, ja šāda informācija tiek lūgta no visām dalībvalstīm.

([1]) Eiropas Parlamenta 2019. gada 12. marta nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2019. gada 9. aprīļa lēmums.
([2]) Padomes Pamatlēmums 2008/675/TI (2008. gada 24. jūlijs) par Eiropas Savienības dalībvalstīs pieņemtu spriedumu ņemšanu vērā jaunā kriminālprocesā (OV L 220, 15.8.2008., 32. lpp.).
([3]) Padomes Pamatlēmums 2009/315/TI (2009. gada 26. februāris) par organizatoriskiem pasākumiem un saturu no sodāmības reģistra iegūtas informācijas apmaiņai starp dalībvalstīm (OV L 93, 7.4.2009., 23. lpp.).
([4]) Padomes Lēmums 2009/316/TI (2009. gada 6. aprīlis) par Eiropas Sodāmības reģistru informācijas sistēmas (*ECRIS*) izveidi, piemērojot Pamatlēmuma 2009/315/TI 11. pantu (OV L 93, 7.4.2009., 33. lpp.).

(6) Šādi vispārējie lūgumi rada nesamērīgu administratīvo slogu visām dalībvalstīm, arī tām, kurām nav informācijas par konkrēto trešās valsts valstspiederīgo. Praksē minētais slogs attur dalībvalstis no lūgumiem sniegt informāciju par trešo valstu valstspiederīgajiem no citām dalībvalstīm, kas ievērojami apgrūtina šādas informācijas apmaiņu starp tām, ierobežojot to piekļuvi sodāmības reģistra informācijai, ļaujot piekļūt informācijai tikai pašu šo valstu reģistrā. Rezultātā palielinās risks, ka informācijas apmaiņa starp dalībvalstīm būs neefektīva un nepilnīga, kas savukārt ietekmē Savienības pilsoņiem un Savienībā dzīvojošām personām nodrošinātās drošības un drošuma līmeni.

(7) Lai šo situāciju uzlabotu, būtu jāizveido sistēma, ar kuras palīdzību dalībvalsts centrālā iestāde var ātri un efektīvi uzzināt, kurām citām dalībvalstīm ir sodāmības reģistra informācija par trešās valsts valstspiederīgo (*"ECRIS-TCN"*). Esošo *ECRIS* tad varētu izmantot, lai lūgtu sodāmības reģistra informāciju no minētajām dalībvalstīm saskaņā ar Pamatlēmumu 2009/315/TI.

(8) Tāpēc šajā regulā būtu jāparedz noteikumi par tādas centralizētas sistēmas izveidi Savienības līmenī, kurā būtu ietverti persondati, un noteikumi par pienākumu sadali starp dalībvalsti un organizāciju, kas atbild par centralizētās sistēmas izstrādi un uzturēšanu, kā arī jebkādi specifiski datu aizsardzības noteikumi, kas ir vajadzīgi, lai papildinātu esošos datu aizsardzības pasākumus un paredzētu adekvātu vispārēju līmeni attiecībā uz datu aizsardzību, datu drošību un attiecīgo personu pamattiesību aizsardzību.

(9) Lai sasniegtu mērķi piedāvāt Savienības pilsoņiem brīvības, drošības un tiesiskuma telpu bez iekšējām robežām, kurā ir nodrošināta personu brīva pārvietošanās, ir vajadzīgs arī, lai informācija par notiesājošiem spriedumiem attiecībā uz Savienības pilsoņiem, kuriem ir arī kādas trešās valsts valstspiederība, būtu pilnīga. Ņemot vērā iespēju, ka šīs personas varētu uzrādīt, ka tām ir viena vai vairākas valstspiederības un ka notiesāšanas dalībvalstī vai valstspiederības dalībvalstī varētu tikt glabāta informācija par dažādiem notiesājošiem spriedumiem, šīs regulas darbības jomā ir jāiekļauj Savienības pilsoņi, kuriem ir arī kādas trešās valsts valstspiederība. Šādu personu izslēgšanas rezultātā *ECRIS-TCN* uzglabātā informācija būtu nepilnīga. Tas apdraudētu sistēmas uzticamību. Tomēr, tā kā šādām personām ir Savienības pilsonība, nosacījumiem, ar kādiem pirkstu nospiedumu datus attiecībā uz šīm personām var iekļaut *ECRIS-TCN*, vajadzētu būt salīdzināmiem ar nosacījumiem, ar kādiem dalībvalstis apmainās ar Savienības pilsoņu pirkstu nospiedumu datiem ar Pamatlēmumu 2009/315/TI un Lēmumu 2009/316/TI izveidotajā *ECRIS*. Tāpēc attiecībā uz Savienības pilsoņiem, kuriem ir arī kādas trešās valsts valstspiederība, pirkstu nospiedumu dati būtu jāiekļauj *ECRIS-TCN* sistēmā tikai tad, ja tie ir iegūti saskaņā ar valsts tiesību aktiem kriminālprocesā, saprotot, ka šādas iekļaušanas sakarā dalībvalstīm vajadzētu būt iespējai izmantot pirkstu nospiedumu datus, kas iegūti citiem mērķiem, kas nav kriminālprocess, ja šāds izmantojums ir atļauts valsts tiesību akti.

(10) *ECRIS-TCN* būtu jāļauj apstrādāt pirkstu nospiedumu dati nolūkā identificēt dalībvalstis, kurām ir sodāmības reģistru informācija par trešās valsts valstspiederīgo. Tai būtu jāļauj apstrādāt arī sejas attēlus nolūkā apstiprināt viņu identitāti. Ir īpaši svarīgi, lai pirkstu nospiedumu dati un sejas attēli tiktu ievadīti un izmantoti tikai tiktāl, cik tas ir stingri nepieciešams attiecīgā mērķa sasniegšanai, lai to ievadē un izmantošanā tiktu ievērotas pamattiesības, kā arī bērna intereses, un lai tie tiktu ievadīti un izmantoti saskaņā ar piemērojamajiem Savienības datu aizsardzības noteikumiem.

(11) Eiropas Savienības Aģentūrai lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/1726 ([5]), būtu jāuztic uzdevums izstrādāt un pārvaldīt *ECRIS-TCN*, ņemot vērā aģentūras pieredzi citu lielapjoma sistēmu pārvaldībā tieslietu un iekšlietu jomā. Aģentūras pilnvaras būtu jāgroza, lai atspoguļotu minētos jaunos uzdevumus.

(12) *eu-LISA* būtu jānodrošina ar pienācīgu finansējumu un personālu, lai tā varētu izpildīt šajā regulā tai paredzētos pienākumus.

(13) Ņemot vērā to, ka ir jāizveido ciešas tehniskas saiknes starp *ECRIS-TCN* un *ECRIS*, *eu-LISA* būtu jāuztic arī uzdevums pilnveidot un uzturēt *ECRIS* ieteicamo īstenošanas programmatūru, un *eu-LISA* pilnvaras būtu jāgroza, lai to atspoguļotu.

(14) Četras dalībvalstis ir izstrādājušas savu valsts *ECRIS* īstenošanas programmatūru saskaņā ar Lēmumu 2009/316/TI un ir to izmantojušas *ECRIS* ieteicamās īstenošanas programmatūras vietā, lai apmainītos ar sodāmības reģistru informāciju. Ņemot vērā konkrētus elementus, ko šīs dalībvalstis savās sistēmās ir ieviesušas savas valsts vajadzībām, un veiktos ieguldījumus, tām būtu jāatļauj izmantot savu valsts *ECRIS* īstenošanas programmatūru arī *ECRIS-TCN* nolūkos, ar noteikumu, ka tiek ievēroti šajā regulā izklāstītie nosacījumi.

([5]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1726 (2018. gada 14. novembris) 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 295, 21.11.2018., 99. lpp.).

(15) *ECRIS-TCN* būtu jāietver tikai to trešo valstu valstspiederīgo identitātes informācija, kuriem kāda krimināltiesa Savienībā pasludinājusi notiesājošu spriedumu. Šādā identitātes informācijā būtu jāiekļauj burtciparu dati un pirkstu nospiedumu dati. Vajadzētu būt arī iespējamai sejas attēlu iekļaušanai, ciktāl tās dalībvalsts, kurā ir pasludināts notiesājošs spriedums, tiesību aktos ir atļauta notiesātas personas sejas attēlu iegūšana un glabāšana.

(16) Burtciparu datos, kas dalībvalstīm jāievada centrālajā sistēmā, būtu jāietver notiesātās personas uzvārds un vārds (vārdi), kā arī, ja centrālajai iestādei šāda informācija ir pieejama – jebkādi minētās personas pseidonīmi vai pieņemtie vārdi. Ja attiecīgajai dalībvalstij ir zināmi citi persondati, kas atšķiras, piemēram, atšķirīgs vārda rakstības veids citā alfabētā, vajadzētu būt iespējai ievadīt šādus datus centrālajā sistēmā kā papildinformāciju.

(17) Burtciparu datos kā papildinformācija būtu jāiekļauj arī identitātes numurs vai personas identifikācijas dokumentu veids un numurs, kā arī attiecīgo dokumentu izdevējiestādes nosaukums, ja šāda informācija centrālajai iestādei ir pieejama. Pirms attiecīgās informācijas ievadīšanas centrālajā sistēmā dalībvalstij būtu jācenšas pārbaudīt identifikācijas dokumentu autentiskumu. Jebkurā gadījumā, tā kā šāda informācija varētu būt neuzticama, tā būtu jāizmanto piesardzīgi.

(18) Centrālajām iestādēm būtu jāizmanto *ECRIS-TCN*, lai identificētu dalībvalstis, kam ir sodāmības reģistra informācija par trešās valsts valstspiederīgo, ja sodāmības reģistru informācija par minēto personu tiek lūgta attiecīgajā dalībvalstī saistībā ar kriminālprocesu pret minēto personu, vai šajā regulā minētajiem nolūkiem. Lai gan *ECRIS-TCN* būtu principā jāizmanto visos šādos gadījumos, iestādei, kas atbild par kriminālprocesa norisi, vajadzētu būt iespējai nolemt, ka *ECRIS-TCN* nebūtu jāizmanto, ja tas nebūtu piemēroti lietas apstākļiem, piemēram, dažos steidzamu kriminālprocesu veidos, lietās, kas saistītas ar tranzītu, ja sodāmības reģistra informācija, izmantojot *ECRIS* iegūta nesen, vai attiecībā uz maznozīmīgiem noziedzīgiem nodarījumiem, jo īpaši sīkiem noziedzīgiem nodarījumiem, pārkāpjot satiksmes noteikumus, maznozīmīgiem noziedzīgiem nodarījumiem, pārkāpjot pašvaldību saistošos noteikumus, un maznozīmīgiem noziedzīgiem nodarījumiem, pārkāpjot sabiedrisko kārtību.

(19) Dalībvalstīm vajadzētu būt iespējai izmantot *ECRIS-TCN* citiem nolūkiem, kas nav noteikti šajā regulā, ja tas ir paredzēts valsts tiesību aktos, un saskaņā ar tiem. Tomēr, lai uzlabotu *ECRIS-TCN* izmantošanas pārredzamību, dalībvalstīm par šādiem citiem nolūkiem būtu jāpaziņo Komisijai, kam būtu jānodrošina visu šo paziņojumu publicēšana *Eiropas Savienības Oficiālajā Vēstnesī*.

(20) Arī citām iestādēm, kas lūdz sniegt informāciju no sodāmības reģistra, vajadzētu būt iespējai nolemt, ka *ECRIS-TCN* nebūtu jāizmanto, ja tas nebūtu piemēroti lietas apstākļos, piemēram, ja ir jāveic konkrētas standarta administratīvās pārbaudes attiecībā uz personas profesionālo kvalifikāciju, jo īpaši, ja ir zināms, ka sodāmības reģistru informācija netiks lūgta no citām dalībvalstīm, neatkarīgi no rezultāta, ko iegūst *ECRIS-TCN* meklēšanas rezultātā. Tomēr *ECRIS-TCN* būtu vienmēr jāizmanto, ja lūgumu sniegt informāciju no sodāmības reģistriem ir ierosinājusi persona, kas lūdz sniegt informāciju par savām sodāmībām saskaņā ar Pamatlēmumu 2009/315/TI, vai ja tas tiek veikts, lai iegūtu sodāmības reģistru informāciju saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 2011/93/ES ([6]).

(21) Trešo valstu valstspiederīgajiem vajadzētu būt tiesībām saņemt rakstisku informāciju par savu sodāmību saskaņā ar tās dalībvalsts tiesību aktiem, kurā viņi lūdz sniegt šādu informāciju, un saskaņā ar Pamatlēmumu 2009/315/TI. Pirms attiecīgā dalībvalsts šādu informāciju sniedz trešās valsts valstspiederīgajam, tai būtu jāveic meklēšana *ECRIS-TCN*.

(22) Savienības pilsoņi, kuriem ir arī kādas trešās valsts valstspiederība, tiks iekļauti *ECRIS-TCN* tikai tad, ja kompetentajām iestādēm ir zināms, ka šādām personām ir kādas trešās valsts valstspiederība. Ja kompetentajām iestādēm nav zināms, ka Savienības pilsoņiem ir arī kādas trešās valsts valstspiederība, tomēr ir iespējams, ka šādām personām ir iepriekšēja sodāmība kā trešās valsts valstspiederīgajiem. Lai nodrošinātu, ka kompetento iestāžu rīcībā ir pilnīgs pārskats par sodāmību, vajadzētu būt iespējai veikt meklēšanu *ECRIS-TCN*, lai pārbaudītu, vai attiecībā uz Savienības pilsoni kādai dalībvalstij ir sodāmības reģistra informācija par šo personu kā trešās valsts valstspiederīgo.

(23) Ja centrālajā sistēmā reģistrētie dati atbilst datiem, kurus, veicot meklēšanu, izmantojusi kāda dalībvalsts (trāpījums), reizē ar trāpījumu tiek sniegta arī identitātes informācija, attiecībā uz kuru ticis reģistrēts trāpījums. Centrālajām iestādēm meklēšanas rezultāts būtu jāizmanto tikai, lai iesniegtu lūgumu, izmantojot *ECRIS*, savukārt, Eiropas Savienības Aģentūrai tiesu iestāžu sadarbībai krimināllietās (*Eurojust*), kas izveidota ar

([6]) Eiropas Parlamenta un Padomes Direktīva 2011/93/ES (2011. gada 13. decembris) par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, un ar kuru aizstāj Padomes Pamatlēmumu 2004/68/TI (OV L 335, 17.12.2011., 1. lpp.).

Eiropas Parlamenta un Padomes Regulu (ES) 2018/1727 ([7]), Eiropas Savienības Aģentūrai tiesībaizsardzības sadarbībai (Eiropols), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/794 ([8]), un Eiropas Prokuratūrai ("*EPPO*"), kas izveidota ar Padomes Regulu (ES) 2017/1939 ([9]), – tikai, lai lūgtu sniegt informāciju par notiesājošajiem spriedumiem, kā minēts šajā regulā.

(24) Sejas attēlus, kuri ietverti *ECRIS-TCN*, sākotnēji būtu jāizmanto tikai trešās valsts valstspiederīgā identitātes apstiprināšanai, lai noteiktu dalībvalstis, kurām ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz minēto trešās valsts valstspiederīgo. Nākotnē vajadzētu būt iespējai sejas attēlus izmantot automatizētai biometrisko datu salīdzināšanai ar noteikumu, ka tiks izpildītas tehniskās un politikas prasības, lai to varētu darīt. Komisijai, ņemot vērā nepieciešamību un samērīgumu, kā arī tehnisko attīstību sejas atpazīšanas programmatūras jomā, būtu jāizvērtē vajadzīgās tehnoloģijas pieejamība un gatavība, pirms pieņemt deleģēto aktu par sejas attēlu izmantošanu nolūkā identificēt trešo valstu valstspiederīgos, lai noteiktu dalībvalstis, kam ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz minētajām personām.

(25) Biometrisko datu izmantošana ir vajadzīga, jo tā ir visuzticamākā metode, lai dalībvalstu teritorijā identificētu trešo valstu valstspiederīgos, kuriem bieži vien nav dokumentu vai nekādu citu identifikācijas līdzekļu, kā arī lai noteiktu ticamāku atbilstību trešo valstu valstspiederīgo datiem.

(26) Dalībvalstīm centrālajā sistēmā būtu jāievada notiesātu trešo valstu valstspiederīgo pirkstu nospiedumu dati, kas saskaņā ar valsts tiesību aktiem iegūti kriminālprocesa gaitā. Lai centrālajā sistēmā būtu pēc iespējas pilnīgāka identitātes informācija, dalībvalstīm vajadzētu būt iespējai centrālajā sistēmā ievadīt arī pirkstu nospiedumu datus, kas iegūti kādiem citiem nolūkiem, kas nav kriminālprocess, ja minētie pirkstu nospiedumu dati ir pieejami izmantošanai kriminālprocesā saskaņā ar valsts tiesību aktiem.

(27) Ar šo regulu būtu jānosaka minimālie kritēriji attiecībā uz pirkstu nospiedumu datiem, kas dalībvalstīm būtu jāiekļauj centrālajā sistēmā. Dalībvalstīm vajadzētu dot izvēli – ievadīt vai nu tādu trešo valstu valstspiederīgo pirkstu nospiedumu datus, kam ir piemērots brīvības atņemšanas sods vismaz uz 6 mēnešiem, vai arī ievadīt tādu trešo valstu valstspiederīgo pirkstu nospiedumu datus, kas ir notiesāti par noziedzīgu nodarījumu, kam saskaņā ar attiecīgās dalībvalsts tiesībām piemērojamais sods paredz brīvības atņemšanu ar maksimālo ilgumu, kas ir vismaz 12 mēneši.

(28) Dalībvalstīm *ECRIS-TCN* būtu jāizveido ieraksti par notiesātiem trešo valstu valstspiederīgajiem. Ja iespējams, tas būtu jādara automātiski, un lieki nekavējoties pēc tam, kad viņus notiesājošie spriedumi reģistrēti valsts sodāmības reģistrā. Dalībvalstīm būtu saskaņā ar šo regulu centrālajā sistēmā jāievada burtciparu un pirkstu nospiedumu dati, kas attiecas uz notiesājošiem spriedumiem, kuri pasludināti pēc dienas, kurā datus sāk ievadīt *ECRIS-TCN*. No tās pašas dienas un jebkurā laikā pēc tam dalībvalstīm vajadzētu būt iespējai centrālajā sistēmā ievadīt sejas attēlus.

(29) Lai nodrošinātu maksimālu sistēmas efektivitāti, dalībvalstīm saskaņā ar šo regulu *ECRIS-TCN* būtu arī jāizveido ieraksti par trešo valstu valstspiederīgajiem, kuri notiesāti pirms dienas, kurā sāk ievadīt datus. Tomēr šajā nolūkā dalībvalstīm nevajadzētu būt pienākumam ievākt informāciju, kas vēl nav to sodāmības reģistros pirms dienas, kurā sāk ievadīt datus. Trešo valstu valstspiederīgo pirkstu nospiedumu dati, kas ievākti saistībā ar šādiem iepriekšējiem notiesājošiem spriedumiem, būtu jāiekļauj tikai tad, ja tie ir iegūti kriminālprocesa gaitā un ja attiecīgā dalībvalsts uzskata, ka var skaidri noteikt to atbilstību citai identitātes informācijai sodāmības reģistros.

(30) Labākai informācijas apmaiņai par notiesājošiem spriedumiem būtu jāpalīdz dalībvalstīm īstenot Pamatlēmumu 2008/675/TI, kurā dalībvalstīm ir uzlikts pienākums jaunā kriminālprocesā ņemt vērā citās dalībvalstīs iepriekš pasludinātus notiesājošus spriedumus, ciktāl attiecīgie valstu iepriekš pasludinātie notiesājošie spriedumi tiek ņemti vērā saskaņā ar attiecīgās valsts tiesību aktiem.

([7]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1727 (2018. gada 14. novembris) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI (OV L 295, 21.11.2018., 138. lpp.).

([8]) 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.).

([9]) Padomes Regula (ES) 2017/1939 (2017. gada 12. oktobris), ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (*EPPO*) izveidei (OV L 283, 31.10.2017., 1. lpp.).

(31) Trāpījumam *ECRIS-TCN* pašam par sevi nebūtu jānozīmē, ka attiecīgais trešās valsts valstspiederīgais bijis notiesāts norādītajās dalībvalstīs. Tas, vai ir bijuši iepriekšēji notiesājoši spriedumi, būtu jāapstiprina tikai, pamatojoties uz informāciju, kas saņemta no attiecīgo dalībvalstu sodāmības reģistriem.

(32) Neraugoties uz iespēju izmantot Savienības finanšu programmas saskaņā ar piemērojamajiem noteikumiem, katrai dalībvalstij būtu jāsedz savas izmaksas, kas rodas no valsts sodāmības reģistra datubāzes un valstu pirkstu nospiedumu datubāzu ieviešanas, pārvaldības, izmantošanas un uzturēšanas, kā arī no to tehnisko pielāgojumu īstenošanas, pārvaldības, izmantošanas un uzturēšanas, kas nepieciešami, lai varētu izmantot *ECRIS-TCN*, tostarp to savienojumus ar valsts centrālo piekļuves punktu.

(33) *Eurojust*, Eiropolam un *EPPO* vajadzētu būt piekļuvei *ECRIS-TCN* sistēmai nolūkā identificēt dalībvalstis), kam ir sodāmības reģistra informācija par kādu trešās valsts valstspiederīgo, lai atbalstītu šīs iestādes tām tiesību aktos noteikto uzdevumu pildīšanā. *Eurojust* arī vajadzētu būt tiešai piekļuvei *ECRIS-TCN* sistēmai, lai pildītu ar šo regulu uzticēto uzdevumu, proti, darboties kā trešo valstu un starptautisku organizāciju kontaktpunktam, neskarot principu par tiesu iestāžu sadarbību krimināllietās, tostarp noteikumu par savstarpēju tiesisko palīdzību, piemērošanu. Lai arī būtu jāņem vērā to dalībvalstu nostāja, kuras nepiedalās ciešākā sadarbībā, ar ko izveido *EPPO*, nebūtu jāatsaka *EPPO* piekļuve informācijai par notiesājošiem spriedumiem tikai tādēļ, ka attiecīgā dalībvalsts nepiedalās ciešākā sadarbībā.

(34) Ar šo regulu nosaka stingrus noteikumus attiecībā uz piekļuvi *ECRIS-TCN* sistēmai un vajadzīgos aizsardzības pasākumus, arī dalībvalstu atbildību par datu vākšanu un izmantošanu. Tajā ir arī noteikts, kā personas var izmantot savas tiesības uz kompensāciju, piekļuvi, labošanu, dzēšanu un pārsūdzību, it īpaši tiesības uz efektīvu tiesību aizsardzību, un ka publiskas neatkarīgas iestādes veic datu apstrādes darbību uzraudzību. Tādējādi tajā ir ievērotas pamattiesības un pamatbrīvības, kas nostiprināti jo īpaši Eiropas Savienības Pamattiesību hartā, tostarp tiesības uz persondatu aizsardzību, vienlīdzības likuma priekšā princips un vispārējais diskriminācijas aizliegums. Šajā sakarā tajā ir ņemta vērā arī Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija, Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām un citi pienākumi cilvēktiesību jomā saskaņā ar starptautiskajām tiesībām.

(35) Persondatu apstrādei, ko kompetentās valsts iestādes veic, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu, būtu jāpiemēro Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 ([10]). Persondatu apstrādei, ko veic valsts iestādes, ja šāda datu apstrāde nav Direktīvas (ES) 2016/680 darbības jomā, būtu jāpiemēro Eiropas Parlamenta un Padomes Regula (ES) 2016/679 ([11]). Būtu jānodrošina koordinēta uzraudzība saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 ([12]), kura būtu jāpiemēro arī persondatu apstrādei, ko veic *eu-LISA*.

(36) Attiecībā uz iepriekšējiem notiesājošiem spriedumiem centrālajām iestādēm burtciparu dati būtu jāievada līdz datu ievadīšanas laikposma beigām saskaņā ar šo regulu un pirkstu nospiedumu dati –divu gadu laikā no dienas, kad sāk darboties *ECRIS-TCN* sistēma. Dalībvalstīm vajadzētu būt iespējai ievadīt visus datus vienlaikus ar noteikumu, ka tiek ievēroti minētie termiņi.

(37) Būtu jāparedz noteikumi par dalībvalstu, *Eurojust*, Eiropola, *EPPO* un *eu-LISA* atbildību attiecībā uz jebkuru kaitējumu, kas radies no šīs regulas pārkāpuma.

(38) Lai uzlabotu to dalībvalstu identificēšanu, kam ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz trešo valstu valstspiederīgajiem, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 290. pantu, lai tā papildinātu šo regulu ar sejas attēlu izmantošanu, nolūkā identificēt trešo valstu valstspiederīgos, kas ļautu noteiktu dalībvalstis, kam ir informācija par iepriekšējiem notiesājošiem spriedumiem. 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

([10]) 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.).

([11]) 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.).

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

2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu ([13]). 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.

(39) Lai nodrošinātu vienādus *ECRIS-TCN* sistēmas izveides un darbības pārvaldības nosacījumus, būtu jāpiešķir īstenošanas pilnvaras Komisijai. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 ([14]).

(40) Dalībvalstīm, cik drīz vien iespējams, būtu jāveic vajadzīgie pasākumi šīs regulas prasību izpildei, lai nodrošinātu *ECRIS-TCN* sistēmas pienācīgu darbību, ņemot vērā laiku, kas *eu-LISA* vajadzīgs *ECRIS-TCN* sistēmas izstrādei un ieviešanai. Tomēr dalībvalstīm šīs regulas īstenošanai vajadzīgo pasākumu veikšanai vajadzētu būt vismaz 36 mēnešiem pēc šīs regulas stāšanās spēkā.

(41) Ņemot vērā to, ka šīs regulas mērķi – proti, panākt ātru un efektīvu precīzas sodāmības reģistru informācijas apmaiņu par trešo valstu valstspiederīgajiem – nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet ka, ieviešot kopīgus noteikumus, minēto mērķi var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai.

(42) 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.

(43) Saskaņā ar 1. un 2. pantu un 4.a panta 1. punktu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots LES un LESD, un neskarot minētā protokola 4. pantu, Īrija nepiedalās šīs regulas pieņemšanā, un šī regula tai nav saistoša un nav jāpiemēro.

(44) Saskaņā ar 3. pantu un 4.a panta 1. punktu Protokolā Nr. 21, Apvienotā Karaliste ir paziņojusi, ka tā vēlas piedalīties šīs regulas pieņemšanā un piemērošanā.

(45) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001 ([15]) 28. panta 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2017. gada 12. decembrī ([16]) sniedza atzinumu,

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

Vispārīgi noteikumi

1. pants

Priekšmets

Ar šo regulu izveido:

a) sistēmu, kā identificēt dalībvalstis, kurām ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz trešo valstu valstspiederīgajiem ("*ECRIS-TCN* sistēma");

b) nosacījumus, saskaņā ar kuriem centrālās iestādes izmanto *ECRIS-TCN* sistēmu, lai iegūtu informāciju par šādiem iepriekšējiem notiesājošiem spriedumiem, izmantojot Eiropas Sodāmības reģistru informācijas sistēmu (*ECRIS*), kas izveidota ar Lēmumu 2009/316/TI, kā arī nosacījumus, saskaņā ar kuriem *Eurojust*, Eiropols un *EPPO* izmanto *ECRIS-TCN* sistēmu.

([13]) OV L 123, 12.5.2016., 1. lpp.
([14]) 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.).
([15]) 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.).
([16]) OV C 55, 14.2.2018., 4. lpp.

2. pants

Darbības joma

Šo regulu piemēro tādu trešo valstu valstspiederīgo identitātes informācijas apstrādei, attiecībā uz kuriem dalībvalstīs ir pasludināti notiesājoši spriedumi, lai identificētu dalībvalstis, kur šādi notiesājoši spriedumi ir pasludināti. Šīs regulas noteikumus, ko piemēro trešo valstu valstspiederīgajiem, – izņemot 5. panta 1. punkta b) apakšpunkta ii) punktu – piemēro arī Savienības pilsoņiem, kuriem ir arī kādas trešās valsts valstspiederība un attiecībā uz kuriem ir pasludināti notiesājoši spriedumi dalībvalstīs.

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "notiesājošs spriedums" ir jebkurš krimināltiesas pieņemts galīgs lēmums, ar ko fizisku personu notiesā par noziedzīgu nodarījumu, ciktāl šāds lēmums ir iekļauts notiesāšanas dalībvalsts sodāmības reģistrā;

2) "kriminālprocess" ir pirmstiesas stadija, tiesas stadija un notiesājošā sprieduma izpilde;

3) "sodāmības reģistrs" ir valsts reģistrs vai reģistri, kuros saskaņā ar valsts tiesību aktiem reģistrē notiesājošus spriedumus;

4) "notiesāšanas dalībvalsts" ir dalībvalsts, kurā ir pasludināts notiesājošs spriedums;

5) "centrālā iestāde" ir iestāde, kas iecelta saskaņā ar Pamatlēmuma 2009/315/TI 3. panta 1. punktu;

6) "kompetentās iestādes" ir centrālās iestādes un *Eurojust*, Eiropols un *EPPO*, kas ir kompetentas piekļūt *ECRIS-TCN* sistēmai vai veikt meklēšanu tajā saskaņā ar šo regulu;

7) "trešās valsts valstspiederīgais" ir persona, kas nav Savienības pilsonis LESD 20. panta 1. punkta nozīmē, vai kas ir bezvalstnieks, vai persona, kuras valstspiederība nav zināma;

8) "centrālā sistēma" ir datubāze vai datubāzes, kuras ir izstrādājusi un uztur *eu-LISA* un kurās ir identitātes informācija par tādiem trešo valstu valstspiederīgajiem, par kuriem dalībvalstīs ir pasludināti notiesājoši spriedumi;

9) "saskarnes programmatūra" ir programmatūra, ko mitina kompetentās iestādes un kas ļauj tām piekļūt centrālajai sistēmai, izmantojot 4. panta 1. punkta d) apakšpunktā minēto komunikācijas infrastruktūru;

10) "identitātes informācija" ir burtciparu dati, pirkstu nospiedumu dati un sejas attēli, ko izmanto, lai noteiktu šo datu saistību ar fizisku personu;

11) "burtciparu dati" ir dati, ko veido burti, cipari, īpašas zīmes, atstarpes un pieturzīmes;

12) "pirkstu nospiedumu dati" ir dati par uzspiestiem un pārveltiem personas katra pirksta nospiedumiem;

13) "sejas attēls" ir digitāls personas sejas attēls;

14) "trāpījums" ir atbilstība vai atbilstības, kuras konstatētas, salīdzinot identitātes informāciju, kas reģistrēta centrālajā sistēmā, un identitātes informāciju, kas izmantota meklēšanai;

15) "valsts centrālais piekļuves punkts" ir valsts pieslēgumpunkts 4. panta 1. punkta d) apakšpunktā minētajai komunikācijas infrastruktūrai;

16) "*ECRIS* ieteicamā īstenošanas programmatūra" ir programmatūra, ko izstrādājusi Komisija un kas darīta pieejama dalībvalstīm, lai apmainītos ar sodāmības reģistra informāciju, izmantojot *ECRIS* sistēmu;

17) "valsts kompetentā iestāde" ir neatkarīga publiska iestāde, ko dalībvalsts izveidojusi, ievērojot piemērojamos Savienības noteikumus datu aizsardzības noteikumus jomā;

18) "uzraudzības iestādes" ir Eiropas Datu aizsardzības uzraudzītājs un valstu uzraudzības iestādes.

4. pants

ECRIS-TCN sistēmas tehniskā arhitektūra

1. *ECRIS-TCN* sistēmu veido:

a) centrālā sistēma, kurā glabā identitātes informācija par notiesātiem trešo valstu valstspiederīgajiem;

b) valsts centrālais piekļuves punkts katrā dalībvalstī;

c) saskarnes programmatūra, kas ļauj kompetentajām iestādēm pieslēgties centrālajai sistēmai, izmantojot valstu centrālos piekļuves punktus un d) apakšpunktā minēto komunikācijas infrastruktūru;

d) komunikācijas infrastruktūra starp centrālo sistēmu un valstu centrālajiem piekļuves punktiem.

2. Centrālo sistēmu mitina *eu-LISA* savos tehniskajos birojos.

3. Saskarnes programmatūru integrē *ECRIS* ieteicamajā īstenošanas programmatūrā. Dalībvalstis izmanto *ECRIS* ieteicamo īstenošanas programmatūru vai – situācijā un atbilstoši nosacījumiem, kas izklāstīti 4. līdz 8. punktā, valsts *ECRIS* īstenošanas programmatūru, – lai veiktu meklēšanu *ECRIS-TCN* sistēmā, un lai nosūtītu papildu lūgumus sniegt sodāmības reģistru informāciju.

4. Dalībvalstis, kas izmanto savu valsts *ECRIS* īstenošanas programmatūru, ir atbildīgas par to, lai nodrošinātu, ka to valsts *ECRIS* īstenošanas programmatūra ļauj to valsts sodāmības reģistru iestādēm saskaņā ar šo regulu izmantot *ECRIS-TCN* sistēmu, izņemot saskarnes programmatūru. Minētajā nolūkā pirms dienas, kad sāk darboties *ECRIS-TCN* sistēma saskaņā ar 35. panta 4. punktu, tās nodrošina, lai to valsts *ECRIS* īstenošanas programmatūra darbotos saskaņā ar protokoliem un tehniskajām specifikācijām, kas noteiktas 10. pantā minētajos īstenošanas aktos, un saskaņā ar jebkādām papildu tehniskajām prasībām, ko nosaka *eu-LISA*, ievērojot šo regulu, kuru pamatā ir minētie īstenošanas akti.

5. Kamēr šīs dalībvalstis neizmanto *ECRIS* ieteicamo īstenošanas programmatūru, dalībvalstis, kas izmanto savu valsts *ECRIS* īstenošanas programmatūru, arī nodrošina, ka to valsts *ECRIS* īstenošanas programmatūrā bez liekas kavēšanās ievieš visus turpmākos tehniskos pielāgojumus, kas vajadzīgi saistībā ar izmaiņām tehniskajās specifikācijās, kuras noteiktas 10. pantā minētajos īstenošanas aktos, vai saistībā ar izmaiņām jebkādās papildu tehniskajās prasībās, ko noteikusi *eu-LISA*, ievērojot šo regulu, kuru pamatā ir minētie īstenošanas akti.

6. Dalībvalstis, kas izmanto savu valsts *ECRIS* īstenošanas programmatūru, sedz visas izmaksas saistībā ar savas valsts *ECRIS* īstenošanas programmatūras ieviešanu, uzturēšanu un turpmāku pilnveidošanu un tās saslēgšanu ar *ECRIS-TCN* sistēmu, izņemot saskarnes programmatūru.

7. Ja kāda dalībvalsts, kas izmanto savu valsts *ECRIS* īstenošanas programmatūru, nespēj izpildīt pienākumus, kas tai noteikti saskaņā ar šo pantu, tai ir pienākums izmantot *ECRIS* ieteicamo īstenošanas programmatūru, tostarp integrēto saskarnes programmatūru, lai lietotu *ECRIS-TCN* sistēmu.

8. Attiecībā uz novērtējumu, kas jāveic Komisijai, ievērojot 36. panta 10. punkta b) apakšpunktu, attiecīgās dalībvalstis Komisijai sniedz visu vajadzīgo informāciju.

II NODAĻA

Datu ievadīšana un izmantošana, ko veic centrālās iestādes

5. pants

Datu ievadīšana *ECRIS-TCN* sistēmā

1. Notiesāšanas dalībvalsts centrālā iestāde izveido datu ierakstu centrālajā sistēmā par katru notiesāto trešās valsts valstspiederīgo. Datu ierakstā ietilpst:

a) attiecībā uz burtciparu datiem:

i) iekļaujamā informācija, izņemot, ja atsevišķos gadījumos šāda informācija centrālajai iestādei nav zināma (obligātā informācija):

— uzvārds,

— vārdi,

— dzimšanas datums,

— dzimšanas vieta (pilsēta un valsts),

— valstspiederība vai valstspiederības,

— dzimums,

— iepriekšējie vārdi, ja tādi ir,

— notiesāšanas dalībvalsts kods;

ii) iekļaujamā informācija, ja sodāmības reģistrā tāda ir ievadīta (fakultatīva informācija):

— vecāku vārdi un uzvārdi;

iii) iekļaujamā informācija, ja centrālajai iestādei tāda ir pieejama (papildinformācija):

— identitātes numurs vai personas identifikācijas dokumentu veids un numurs, kā arī izdevējiestādes nosaukums,

— pseidonīmi vai pieņemtie vārdi;

b) attiecībā uz pirkstu nospiedumu datiem:

i) pirkstu nospiedumu dati, kas saskaņā ar valsts tiesību aktiem iegūti kriminālprocesa gaitā;

ii) vismaz tie pirkstu nospiedumu dati, kas iegūti pamatojoties uz jebkuru no šiem kritērijiem:

— ja trešās valsts valstspiederīgajam ir piemērots brīvības atņemšanas sods vismaz uz sešiem mēnešiem

vai

— trešās valsts valstspiederīgais ir notiesāts par noziedzīgu nodarījumu, kam saskaņā ar dalībvalsts tiesību aktiem piemērojamais sods paredz brīvības atņemšanu ar maksimālo ilgumu, kas ir vismaz 12 mēneši.

2. Pirkstu nospiedumu datiem, kas minēti šā panta 1. punkta b) apakšpunktā, ir pirkstu nospiedumu datu kvalitātes, izšķirtspējas un apstrādes tehniskās specifikācijas, kas noteiktas īstenošanas aktā, kas minēts 10. panta 1. punkta b) apakšpunktā. Notiesātās personas pirkstu nospiedumu datu atsauces numurs ietver notiesāšanas dalībvalsts kodu.

3. Datu ierakstā var būt iekļauti arī notiesātā trešās valsts valstspiederīgā sejas attēli, ja notiesāšanas dalībvalsts tiesību aktos ir atļauta notiesāto personu sejas attēlu vākšana un glabāšana.

4. Notiesāšanas dalībvalsts datu ierakstu izveido automātiski, ja iespējams, un bez liekas kavēšanās pēc tam, kad notiesājošais spriedums ir ievadīts sodāmības reģistrā.

5. Notiesāšanas dalībvalstis arī izveido datu ierakstus par notiesājošiem spriedumiem, kas pasludināti pirms datu ievadīšanas sākuma datuma saskaņā ar 35. panta 1. punktu, ciktāl to valsts datubāzēs tiek glabāti dati par notiesātām personām. Šādos gadījumos pirkstu nospiedumi būtu jāiekļauj tikai tad, ja tie ir iegūti kriminālprocesa gaitā saskaņā ar valsts tiesību aktiem un ja var skaidri noteikt to atbilstību citai identitātes informācijai sodāmības reģistros.

6. Lai izpildītu pienākumus, kas izklāstīti 1. punkta b) apakšpunkta i) un ii) punktā un 5. punktā, dalībvalstis var izmantot pirkstu nospiedumu datus, kas iegūti citiem mērķiem, kas nav kriminālprocess, ja šāda izmantošana ir pieļaujama saskaņā ar valsts tiesību aktiem.

6. pants

Sejas attēli

1. Līdz brīdim, kad stājas spēkā deleģētais akts, kas paredzēts 2. punktā, sejas attēlus var izmantot tikai, lai apstiprinātu trešās valsts valstspiederīgā identitāti, ja viņš ir identificēts, burtciparu meklēšanas vai meklēšanas, izmantojot pirkstu nospiedumu datus, rezultātā.

2. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 37. pantu, ar kuriem papildina šo regulu attiecībā uz sejas attēlu izmantošanu nolūkā identificēt trešo valstu valstspiederīgos, lai noteiktu dalībvalstis, kam ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz šādām personām, kad tas kļūst tehniski iespējams. Pirms īstenot šīs pilnvaras, Komisija, ņemot vērā nepieciešamību un samērīgumu, kā arī tehnisko attīstību sejas attēlu atpazīšanas programmatūras jomā, novērtē vajadzīgās tehnoloģijas pieejamību un gatavību.

7. pants

ECRIS-TCN sistēmas izmantošana ar mērķi identificēt dalībvalstis, kurām ir sodāmības reģistru informācija

1. Centrālās iestādes izmanto *ECRIS-TCN* sistēmu, lai identificētu dalībvalstis, kam ir sodāmības reģistru informācija par trešās valsts valstspiederīgo, lai, izmantojot *ECRIS*, iegūtu informāciju par iepriekšējiem notiesājošiem spriedumiem, ja sodāmības reģistru informācija par minēto personu tiek lūgta attiecīgajā dalībvalstī saistībā ar kriminālprocesu pret minēto personu vai jebkuriem šādiem nolūkiem, ja tas ir paredzēts valsts tiesību aktos un saskaņā ar tiem:

— pašas personas sodāmības reģistra informācijas pārbaude pēc paša lūguma,

— drošības pielaide,

— licences vai atļaujas iegūšana,

— pārbaudes pirms pieņemšanas darbā,

— pārbaudes attiecībā uz profesionālu vai organizētu brīvprātīgu darbību, kas ietver tiešu un regulāru saskarsmi ar bērniem vai neaizsargātām personām,

— vīzu, pilsonības iegūšanas un migrācijas procedūras, tostarp patvēruma procedūras, un

— pārbaudes saistībā ar publiskā iepirkuma līgumiem un publisku izskatīšanu.

Tomēr konkrētos gadījumos, kas nav gadījumi, kad trešās valsts valstspiederīgais centrālajai iestādei lūdz informāciju par savām sodāmībām vai kad šāds lūgums ir iesniegts, lai iegūtu sodāmības reģistru informāciju, ievērojot Direktīvas 2011/93/ES 10. panta 2. punktu, iestāde, kas lūdz sniegt informāciju no sodāmības reģistriem, var nolemt, ka šāda *ECRIS-TCN* sistēmas izmantošana nav piemērota.

2. Jebkura dalībvalsts, kas nolemj – ja tas ir paredzēts valsts tiesību aktos, un saskaņā ar tiem – izmantot *ECRIS-TCN* sistēmu citiem nolūkiem, kuri nav izklāstīti 1. punktā, lai, izmantojot *ECRIS*, iegūtu informāciju par iepriekšējiem notiesājošiem spriedumiem, līdz darbības uzsākšanas dienai, kā minēts 35. panta 4. punktā, vai jebkurā laikā pēc tam paziņo Komisijai par šādiem citiem nolūkiem un jebkurām izmaiņām attiecībā uz šādiem nolūkiem. Šādus paziņojumus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī* 30 dienu laikā pēc paziņojumu saņemšanas.

3. *Eurojust*, Eiropols un *EPPO* var veikt meklēšanu *ECRIS-TCN* sistēmā, lai identificētu dalībvalstis, kam ir sodāmības reģistru informācija par kādu trešās valsts valstspiederīgo, saskaņā ar 14. līdz 18. pantu. Bet tās neievada, nelabo un nedzēš *ECRIS-TCN* sistēmā nekādus datus.

4. Nolūkiem, kas minēti 1., 2. un 3. punktā, kompetentās iestādes var arī veikt meklēšanu *ECRIS-TCN* sistēmā, lai pārbaudītu, vai attiecībā uz Savienības pilsoni, kādai dalībvalstij ir sodāmības reģistru informācija par šo personu kā trešās valsts valstspiederīgo.

5. Veicot meklēšanu *ECRIS-TCN* sistēmā, kompetentās iestādes var izmantot visus 5. panta 1. punktā minētos datus vai tikai dažus no tiem. Minimālo datu kopumu, kas vajadzīgs, lai veiktu meklēšanu sistēmā, nosaka īstenošanas aktā, ko pieņem saskaņā ar 10. panta 1. punkta g) apakšpunktu.

6. Kompetentās iestādes var veikt meklēšanu *ECRIS-TCN* sistēmā, arī izmantojot sejas attēlus, ar noteikumu, ka šāda funkcionalitāte ir ieviesta saskaņā ar 6. panta 2. punktu.

7. Trāpījuma gadījumā centrālā sistēma automātiski sniedz kompetentajai iestādei informāciju par dalībvalstīm, kam ir sodāmības reģistru informācija par trešās valsts valstspiederīgo, kā arī ar to saistītos atsauces numurus un jebkādu atbilstošu identitātes informāciju. Šādu identitātes informāciju izmanto tikai, lai pārbaudītu attiecīgā trešās valsts valstspiederīgā identitāti. Rezultātu, kas iegūts, veicot meklēšanu centrālajā sistēmā, var izmantot tikai, lai iesniegtu lūgumu saskaņā ar Pamatlēmuma 2009/315/TI 6. pantu vai lūgumu, kas minēts šīs regulas 17. panta 3. punktā.

8. Ja trāpījums netiek iegūts, centrālā sistēma par to automātiski informē kompetento iestādi.

III NODAĻA

Datu saglabāšana un grozīšana

8. pants

Saglabāšanas periods datu glabāšanai

1. Katru datu ierakstu centrālajā sistēmā glabā tik ilgi, kamēr sodāmības reģistros uzglabā datus, kas saistīti ar attiecīgo personu notiesājošiem spriedumiem.

2. Beidzoties 1. punktā minētajam saglabāšanas periodam, notiesāšanas dalībvalsts centrālā iestāde no centrālās sistēmas dzēš attiecīgo datu ierakstu, tostarp visus pirkstu nospiedumu datus vai sejas attēlus. Dzēšana notiek, ja tas iespējams, automātiski, un jebkurā gadījumā ne vēlāk kā vienu mēnesi pēc tam, kad beidzies saglabāšanas periods.

9. pants

Datu grozīšana un dzēšana

1. Dalībvalstis var grozīt vai dzēst datus, kuros tās ir ievadījušas *ECRIS-TCN* sistēmā.

2. Ja tiek veikti jebkādi grozījumi sodāmības reģistru informācijā, pamatojoties uz kuru saskaņā ar 5. pantu ir izveidots datu ieraksts, notiesāšanas dalībvalsts bez liekas kavēšanās veic identiskus grozījumus informācijā, kas glabājas minētajā datu ierakstā centrālajā sistēmā.

3. Ja notiesāšanas dalībvalstij ir iemesls uzskatīt, ka dati, ko tā ir ievadījusi centrālajā sistēmā, ir neprecīzi vai ka dati centrālajā sistēmā ir apstrādāti, pārkāpjot šo regulu, tā:

a) nekavējoties sāk procedūru attiecīgo datu precizitātes vai attiecīgā gadījumā to apstrādes likumīguma pārbaudei;

b) vajadzības gadījumā bez liekas kavēšanās datus labo vai dzēš no centrālās sistēmas.

4. Ja dalībvalstij, kas nav notiesāšanas dalībvalsts, kura datus ievadījusi, ir iemesls uzskatīt, ka centrālajā sistēmā reģistrētie dati ir neprecīzi vai ka dati centrālajā sistēmā ir apstrādāti, pārkāpjot šo regulu, tā bez liekas kavēšanās sazinās ar notiesāšanas dalībvalsts centrālo iestādi.

Notiesāšanas dalībvalsts:

a) nekavējoties sāk procedūru attiecīgo datu precizitātes vai attiecīgā gadījumā to apstrādes likumīguma pārbaudei;

b) vajadzības gadījumā bez liekas kavēšanās tos labo vai dzēš no centrālās sistēmas;

c) bez liekas kavēšanās informē attiecīgo citu dalībvalsti par to, ka dati ir laboti vai dzēsti, vai par iemesliem, kāpēc dati nav laboti vai dzēsti.

IV NODAĻA

Izstrāde, darbība un pienākumi

10. pants

Īstenošanas akti, ko pieņem Komisija

1. Komisija iespējami drīz pieņem īstenošanas aktus, kas nepieciešami, lai tehniski izstrādātu un ieviestu *ECRIS-TCN* sistēmu, un jo īpaši aktus par:

a) tehniskajām specifikācijām attiecībā uz burtciparu datu apstrādi;

b) tehniskajām specifikācijām, kas attiecas uz pirkstu nospiedumu datu kvalitāti, izšķirtspēju un apstrādi;

c) tehniskajām specifikācijām attiecībā uz saskarnes programmatūru;

d) tehniskajām specifikācijām attiecībā uz sejas attēlu kvalitāti, izšķirtspēju un apstrādi 6. pantā minētajos nolūkos un saskaņā ar tajā izklāstītajiem nosacījumiem;

e) datu kvalitāti, tostarp par mehānismu un procedūrām datu kvalitātes pārbaudes veikšanai;

f) datu ievadīšanu saskaņā ar 5. pantu;

g) piekļuvi *ECRIS-TCN* sistēmai un meklēšanu tajā saskaņā ar 7. pantu;

h) datu grozīšanu un dzēšanu saskaņā ar 8. un 9. pantu;

i) ierakstu glabāšanu un piekļuvi tiem saskaņā ar 31. pantu;

j) centrālā repozitorija darbību un datu drošības un datu aizsardzības noteikumiem, kas piemērojami repozitorijam, saskaņā ar 32. pantu;

k) statistikas nodrošināšanu saskaņā ar 32. pantu;

l) veiktspējas un pieejamības prasībām attiecībā uz *ECRIS-TCN* sistēmu, tostarp minimālajām specifikācijām un prasībām attiecībā uz *ECRIS-TCN* sistēmas biometrisko veiktspēju, jo īpaši saistībā ar vajadzīgo kļūdaini pozitīvas identificēšanas īpatsvaru un kļūdaini negatīvas identificēšanas īpatsvaru.

2. Šā panta 1. punktā minētos īstenošanas aktus pieņem saskaņā ar 38. panta 2. punktā minēto pārbaudes procedūru.

11. pants

ECRIS-TCN sistēmas izstrāde un darbības pārvaldība

1. *eu-LISA* atbild par *ECRIS-TCN* sistēmas izstrādi, ņemot vērā principu, kas paredz integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma. Turklāt *eu-LISA* atbild par *ECRIS-TCN* sistēmas darbības pārvaldību. Izstrāde sastāv no tehnisko specifikāciju izstrādes un ieviešanas, testēšanas un projekta vispārējās koordinācijas.

2. *eu-LISA* atbild arī par *ECRIS* ieteicamās īstenošanas programmatūras turpmāku izstrādi un uzturēšanu.

3. *eu-LISA* nosaka *ECRIS-TCN* sistēmas fiziskās arhitektūras projektu, tostarp tās tehniskās specifikācijas un to attīstību attiecībā uz centrālo sistēmu, valsts centrālo piekļuves punktu un saskarnes programmatūru. Šo projektu pieņem valde, ja ir saņemts labvēlīgs Komisijas atzinums.

4. Pēc šīs regulas stāšanās spēkā un pēc tam, kad Komisija ir pieņēmusi 10. pantā minētos īstenošanas aktus, *eu-LISA* pēc iespējas ātrāk izstrādā un īsteno *ECRIS-TCN* sistēmu.

5. Pirms *ECRIS-TCN* sistēmas plānošanas un izstrādes posma *eu-LISA* valde izveido programmas vadības valdi, kuras sastāvā ir desmit locekļi.

Programmas valdes sastāvā ir astoņi valdes iecelti locekļi, 39. pantā minētās padomdevēju grupas priekšsēdētājs un viens Komisijas iecelts loceklis. Valdes ieceltos locekļus ievēl tikai no tām dalībvalstīm, kurām saskaņā ar Savienības tiesību aktiem ir pilnībā saistoši leģislatīvie instrumenti, ar ko reglamentē *ECRIS*, un kuras piedalīsies *ECRIS-TCN* sistēmā. Valde nodrošina, ka tās ieceltajiem programmas valdes locekļiem ir nepieciešamā pieredze un zināšanas tiesu un sodāmības reģistra iestāžu izmantotu IT sistēmu izstrādē un pārvaldībā.

eu-LISA piedalās programmas valdes darbā. Minētajā nolūkā *eu-LISA* pārstāvji piedalās programmas valdes sanāksmēs, lai ziņotu par darbu pie *ECRIS-TCN* sistēmas plānošanas un izstrādes un par jebkādu citu ar to saistītu darbu un darbībām.

Programmas valde tiekas vismaz reizi trijos mēnešos un biežāk, ja tas ir nepieciešams. Tā nodrošina *ECRIS-TCN* sistēmas plānošanas un izstrādes posma adekvātu pārvaldību un nodrošina konsekvenci starp centrālajiem un valstu *ECRIS-TCN* projektiem un valsts *ECRIS* īstenošanas programmatūru. Programmas valde regulāri – ja iespējams, katru mēnesi – *eu-LISA* valdei iesniedz rakstiskus ziņojumus par projekta progresu. Programmas valdei nav lēmumu pieņemšanas pilnvaru, nedz arī pilnvaru pārstāvēt valdes locekļus.

6. Programmas valde nosaka savu reglamentu, kurā jo īpaši iekļauj noteikumus par:

a) priekšsēdētāju;

b) sanāksmju vietām;

c) sanāksmju sagatavošanu;

d) ekspertu pielaidi sanāksmēm;

e) saziņas plāniem, kas nodrošina to, ka klāt neesoši valdes locekļi tiek pilnībā informēti.

7. Programmas valdes priekšsēdētāja vietu ieņem dalībvalsts, kurai saskaņā ar Savienības tiesību aktiem ir pilnībā saistoši leģislatīvie instrumenti, ar ko reglamentē *ECRIS*, un leģislatīvie instrumenti, ar kuriem reglamentē visu to lielapjoma IT sistēmu izstrādi, izveidi, darbību un izmantošanu, kuras pārvalda *eu-LISA*.

8. Visus ceļošanas un uzturēšanās izdevumus, kas rodas programmas valdes locekļiem, sedz *eu-LISA*. *eu-LISA* reglamenta 10. pantu piemēro mutatis mutandis. Programmas valdes sekretariātu nodrošina *eu-LISA*.

9. Plānošanas un izstrādes posmā 39. pantā minētās padomdevēju grupas sastāvā ir valstu *ECRIS-TCN* sistēmas projektu vadītāji, un to vada *eu-LISA*. Plānošanas un izstrādes posmā grupa sanāk regulāri – ja iespējams, vismaz reizi mēnesī – līdz *ECRIS-TCN* sistēmas darbības sākumam. Pēc katras sanāksmes tā ziņo programmas valdei. Tā nodrošina tehniskās zināšanas, lai atbalstītu programmas valdi uzdevumu veikšanā, un seko līdzi dalībvalstu gatavības stāvoklim.

10. Lai jebkurā laikā nodrošinātu *ECRIS-TCN* sistēmā glabāto datu konfidencialitāti un integritāti, *eu-LISA* sadarbībā ar dalībvalstīm paredz atbilstošus tehniskus un organizatoriskus pasākumus, ņemot vērā tehnoloģijas attīstības līmeni, īstenošanas izmaksas un apstrādes radītos riskus.

11. *eu-LISA* atbild par šādiem uzdevumiem, kas saistīti ar 4. panta 1. punkta d) apakšpunktā minēto komunikācijas infrastruktūru:

a) uzraudzība;

b) drošība;

c) attiecību koordinēšana starp dalībvalstīm un komunikācijas infrastruktūras sniedzēju.

12. Komisija ir atbildīga par visiem pārējiem uzdevumiem, kas saistīti ar 4. panta 1. punkta d) apakšpunktā minēto komunikācijas infrastruktūru, jo īpaši:

a) uzdevumiem saistībā ar budžeta izpildi;

b) iegādi un atjaunošanu;

c) jautājumiem, kas saistīti ar līgumiem.

13. *eu-LISA* izstrādā un uztur mehānismu un procedūras, saskaņā ar kurām jāveic *ECRIS-TCN* sistēmā glabāto datu kvalitātes pārbaudes, un regulāri sniedz ziņojumus dalībvalstīm. *eu-LISA* regulāri sniedz ziņojumus Komisijai par konstatētajām problēmām un attiecīgajām dalībvalstīm.

14. *ECRIS-TCN* sistēmas darbības pārvaldība ir visi tie uzdevumi, kas vajadzīgi, lai nodrošinātu *ECRIS-TCN* sistēmas darbību saskaņā ar šo regulu, it īpaši uzturēšanas darbi un tehniska pielāgošana, kas vajadzīga, lai *ECRIS-TCN* sistēma darbotos apmierinoši saskaņā ar tehniskajām specifikācijām.

15. *eu-LISA* veic uzdevumus, kas saistīti ar apmācības sniegšanu par *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras tehnisko izmantošanu.

16. Neskarot 17. pantu Eiropas Savienības Civildienesta noteikumos, kas noteikti Padomes Regulā (EEK, Euratom, EOTK) Nr. 259/68 ([17]), *eu-LISA* piemēro attiecīgus noteikumus par dienesta noslēpumu vai citas līdzvērtīgas konfidencialitātes prasības visiem saviem darbiniekiem, kam jāstrādā ar centrālajā sistēmā reģistrētiem datiem. Šis pienākums ir spēkā arī tad, kad šie darbinieki vairs nav attiecīgajā amatā vai darbā vai pēc tam, kad viņi ir izbeiguši darbības.

12. pants

Dalībvalstu pienākumi

1. Katra dalībvalsts ir atbildīga par:

a) droša savienojuma nodrošināšanu starp savu valsts sodāmības reģistru un pirkstu nospiedumu datubāzēm un valsts centrālo piekļuves punktu;

b) šā punkta a) apakšpunktā minētā savienojuma izstrādi, darbību un uzturēšanu;

c) savienojuma nodrošināšanu starp savām valsts sistēmām un *ECRIS* ieteicamo īstenošanas programmatūru;

([17]) OV L 56, 4.3.1968., 1. lpp.

d) centrālo iestāžu pienācīgi pilnvarotu darbinieku piekļuves *ECRIS-TCN* sistēmai pārvaldību un organizēšanu saskaņā ar šo regulu un šo darbinieku saraksta un 19. panta 3. punkta g) apakšpunktā minēto profilu izveidi un regulāru atjaunināšanu.

2. Katra dalībvalsts savas centrālās iestādes darbiniekiem, kuriem ir tiesības piekļūt *ECRIS-TCN* sistēmai, nodrošina pienācīgu apmācību, kas jo īpaši aptver datu drošības un datu aizsardzības noteikumus un piemērojamās pamattiesības, pirms viņiem atļauj apstrādāt datus, kas glabājas centrālajā sistēmā.

13. pants

Atbildība par datu izmantošanu

1. Saskaņā ar piemērojamajiem Savienības datu aizsardzības noteikumiem katra dalībvalsts nodrošina, ka *ECRIS-TCN* sistēmā reģistrētos datus apstrādā likumīgi, un jo īpaši to, ka:

a) piekļuve datiem ir tikai pienācīgi pilnvarotiem darbiniekiem viņu uzdevumu veikšanai;

b) datus vāc likumīgi un pilnībā ievērojot trešās valsts valstspiederīgā cilvēka cieņu un pamattiesības;

c) dati *ECRIS-TCN* sistēmā ir ievadīti likumīgi;

d) dati, kad tos ievada *ECRIS-TCN* sistēmā, ir precīzi un aktuāli.

2. *eu-LISA* nodrošina, ka *ECRIS-TCN* sistēma tiek izmantota saskaņā ar šo regulu, 6. panta 2. punktā minēto deleģēto aktu un īstenošanas aktiem, kas minēti 10. pantā, kā arī saskaņā ar Regulu (ES) 2018/1725. Jo īpaši *eu-LISA* veic vajadzīgos pasākumus, lai nodrošinātu centrālās sistēmas un 4. panta 1. punkta d) apakšpunktā minētās komunikācijas infrastruktūras drošību, neskarot katras dalībvalsts atbildību.

3. Par pasākumiem, kurus *eu-LISA* veic saskaņā ar 2. punktu, lai uzsāktu *ECRIS-TCN* sistēmas darbību, tā iespējami īsā laikā pēc šādu pasākumu veikšanas informē Eiropas Parlamentu, Padomi un Komisiju, kā arī Eiropas Datu aizsardzības uzraudzītāju.

4. Komisija 3. punktā minēto informāciju dara pieejamu dalībvalstīm un sabiedrībai, izmantojot regulāri atjauninātu publisku tīmekļa vietni.

14. pants

***Eurojust*, Eiropola un *EPPO* piekļuve sistēmai**

1. Ar mērķi identificēt dalībvalstis, kam ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz trešo valstu valstspiederīgajiem, *Eurojust* ir tieša piekļuve *ECRIS-TCN* sistēmai 17. panta īstenošanas nolūkā, kā arī lai veiktu savus uzdevumus, kā tas minēts Regulas (ES) 2018/1727 2. pantā.

2. Ar mērķi identificēt dalībvalstis, kam ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz trešo valstu valstspiederīgajiem, Eiropolam ir tieša piekļuve *ECRIS-TCN* sistēmai, lai veiktu savus uzdevumus, kā tas minēts Regulas (ES) 2016/794 4. panta 1. punkta e) un h) apakšpunktā.

3. Ar mērķi identificēt dalībvalstis, kam ir informācija par iepriekšējiem notiesājošiem spriedumiem attiecībā uz trešo valstu valstspiederīgajiem, *EPPO* ir tieša piekļuve *ECRIS-TCN* sistēmai, lai veiktu savus uzdevumus, kā tas minēts Regulas (ES) 2017/1939 4. pantā.

4. Ja ir iegūts trāpījums, kurā norādītas dalībvalstis, kam ir sodāmības reģistra informācija par kādu trešās valsts valstspiederīgo, *Eurojust*, Eiropols un *EPPO* var, ievērojot to saziņas veidu, kas noteikts to dibināšanas aktos, sazināties ar attiecīgo dalībvalstu valstu iestādēm, lai lūgtu informāciju no sodāmības reģistriem.

15. pants

***Eurojust*, Eiropola un *EPPO* pilnvarotu darbinieku piekļuve**

Eurojust, Eiropols un *EPPO* ir atbildīgi par pienācīgi pilnvarotu darbinieku piekļuves *ECRIS-TCN* sistēmai pārvaldīšanu un kārtību saskaņā ar šo regulu; un par šādu darbinieku saraksta un viņu profilu izveidi un regulāru atjaunināšanu.

16. pants

Eurojust, Eiropola un _EPPO_ pienākumi

Eurojust, Eiropols un *EPPO*:

a) nodrošina tehniskos līdzekļus, ar kuriem pieslēgties *ECRIS-TCN* sistēmai, un ir atbildīgi par minētā pieslēguma uzturēšanu;

b) tiem saviem darbiniekiem, kuriem ir tiesības piekļūt *ECRIS-TCN* sistēmai, nodrošina atbilstošu apmācību, kas jo īpaši aptver datu drošības un datu aizsardzības noteikumus un piemērojamās pamattiesības, pirms viņiem atļauj apstrādāt datus, kas glabājas centrālajā sistēmā;

c) nodrošina, ka persondati, ko tie apstrādā saskaņā ar šo regulu, ir aizsargāti saskaņā ar piemērojamajiem datu aizsardzības noteikumiem.

17. pants

Trešām valstīm un starptautiskām organizācijām paredzēts kontaktpunkts

1. Trešās valstis un starptautiskas organizācijas krimināprocesa vajadzībām var vērsties pie *Eurojust* ar lūgumiem sniegt informāciju par to, kurām dalībvalstīm (ja tādas ir) ir sodāmības reģistru informācija par kādas trešās valsts valstspiederīgo. Šajā nolūkā tās izmanto šīs regulas pielikumā iekļauto standartveidlapu.

2. Kad *Eurojust* saņem lūgumu saskaņā ar 1. punktu, tā izmanto *ECRIS-TCN* sistēmu, lai noteiktu, kurām dalībvalstīm (ja tādas ir) ir sodāmības reģistru informācija par attiecīgo trešās valsts valstspiederīgo.

3. Ja ir iegūts trāpījums, *Eurojust* vēršas pie dalībvalsts, kam ir sodāmības reģistru informācija par attiecīgo trešās valsts valstspiederīgo, lai noskaidrotu, vai tā piekrīt, ka *Eurojust* trešai valstij vai starptautiskajai organizācijai dara zināmu attiecīgās dalībvalsts nosaukumu. Ja attiecīgā dalībvalsts dod savu piekrišanu, *Eurojust* trešai valstij vai starptautiskajai organizācijai dara zināmu attiecīgās dalībvalsts nosaukumu, un informē trešo valsti vai starptautisko organizāciju par to, kādā veidā tā saskaņā ar piemērojamām procedūrām var iesniegt lūgumu minētajai dalībvalstij, lai iegūtu informāciju no sodāmības reģistra.

4. Gadījumos, kad nav iegūts trāpījums vai ja *Eurojust* nevar sniegt atbildi saskaņā ar 3. punktu uz lūgumiem, kas iesniegti saskaņā ar šo pantu, tā informē attiecīgo trešo valsti vai starptautisko organizāciju, ka tā ir pabeigusi procedūru, nesniedzot nekādu norādi par to, vai sodāmības reģistru informācija par attiecīgo personu ir kādai no dalībvalstīm.

18. pants

Informācijas sniegšana trešai valstij, starptautiskai organizācijai vai privātai struktūrai

Ne *Eurojust*, Eiropols, *EPPO*, ne arī kāda centrālā iestāde nenodod un nedara pieejamus trešai valstij, starptautiskai organizācijai vai privātai struktūrai informāciju, kas iegūta no *ECRIS-TCN* sistēmas par trešās valsts valstspiederīgo. Šis pants neskar 17. panta 3. punktu.

19. pants

Datu drošība

1. *eu-LISA* veic vajadzīgos pasākumus, lai nodrošinātu *ECRIS-TCN* sistēmas drošību, neskarot katras dalībvalsts atbildību un ņemot vērā 3. punktā noteiktos drošības pasākumus.

2. Attiecībā uz *ECRIS-TCN* sistēmas darbību *eu-LISA* veic vajadzīgos pasākumus, lai sasniegtu 3. punktā izklāstītos mērķus, tostarp pieņem drošības plānu un plānu darbības nepārtrauktībai un datu atgūšanai ārkārtas situācijās, un lai nodrošinātu, ka uzstādītās sistēmas traucējumu gadījumā var atjaunot.

3. Dalībvalstis nodrošina datu drošību pirms to pārsūtīšanas uz valsts centrālo piekļuves punktu un to pārsūtīšanas laikā, kā arī saņemot datus no valsts centrālā piekļuves punkta. Jo īpaši, katra dalībvalsts:

a) fiziski aizsargā datus, tostarp izstrādājot ārkārtas rīcības plānus infrastruktūras aizsardzībai;

b) liedz nepilnvarotām personām piekļuvi valsts iekārtām, kurās dalībvalsts veic ar *ECRIS-TCN* sistēmu saistītas darbības;

c) nepieļauj datu neatļautu nolasīšanu, kopēšanu, grozīšanu vai datu nesēju izņemšanu;

d) novērš datu neatļautu ievadīšanu un glabāto persondatu neatļautu apskati, grozīšanu vai dzēšanu;

e) novērš datu neatļautu apstrādi *ECRIS-TCN* sistēmā, kā arī *ECRIS-TCN* sistēmā apstrādātu datu neatļautu grozīšanu vai dzēšanu;

f) nodrošina, ka personām, kas ir pilnvarotas piekļūt *ECRIS-TCN* sistēmai, ir piekļuve tikai tiem datiem, uz kuriem attiecas viņu piekļuves tiesības, izmantojot tikai individuālas lietotāju identitātes un konfidenciālus piekļuves režīmus;

g) nodrošina, ka visas iestādes, kurām ir tiesības piekļūt *ECRIS-TCN* sistēmai, izveido aprakstus par tādu personu amata pienākumiem un atbildības jomām, kurām ir tiesības ievadīt, labot, dzēst, aplūkot un meklēt datus, un bez liekas kavēšanās dara šos aprakstus pieejamus valsts uzraudzības iestādēm pēc to pieprasījuma;

h) nodrošina to, ka ir iespējams pārbaudīt un noteikt, kurām Savienības struktūrām, birojiem un aģentūrām persondatus var pārsūtīt, izmantojot datu pārraides ierīces;

i) nodrošina iespēju pārbaudīt un noteikt, kādi dati ir apstrādāti *ECRIS-TCN* sistēmā, kad, kas un kādam mērķim tos ir apstrādājis;

j) nodrošina, jo īpaši ar pienācīgu šifrēšanas paņēmienu palīdzību, ka laikā, kad persondatus pārsūta uz *ECRIS-TCN* sistēmu vai no tās, vai datu nesēju transportēšanas laikā tos nevar neatļauti nolasīt, kopēt, grozīt vai dzēst;

k) uzrauga šajā punktā minēto drošības pasākumu efektivitāti un veic vajadzīgos organizatoriskos pasākumus saistībā ar pašuzraudzību un pārraudzību, lai nodrošinātu atbilstību šai regulai.

4. *eu-LISA* un dalībvalstis sadarbojas, lai nodrošinātu konsekventu pieeju datu drošībai, pamatojoties uz drošības risku pārvaldības procesu, kas aptver visu *ECRIS-TCN* sistēmu.

20. pants

Atbildība

1. Jebkurai personai vai dalībvalstij, kam nodarīts materiāls vai nemateriāls kaitējums saistībā ar nelikumīgu apstrādes darbību vai citas ar šo regulu nesavienojamas rīcības rezultātā, ir tiesības saņemt kompensāciju no:

a) tās dalībvalsts, kura ir atbildīga par nodarīto kaitējumu; vai

b) *eu-LISA*, gadījumā, ja *eu-LISA* nav ievērojusi šajā regulā vai Regulā (ES) 2018/1725 tai paredzētos pienākumus.

Dalībvalsti, kura ir atbildīga par nodarīto kaitējumu, vai attiecīgi *eu-LISA* pilnībā vai daļēji atbrīvo no atbildības, ja tā pierāda, ka nav atbildīga par notikumu, kas izraisījis šo kaitējumu.

2. Ja saistībā ar to, ka kāda dalībvalsts, *Eurojust*, Eiropols vai *EPPO* nav ievērojusi savus pienākumus saskaņā ar šo regulu, ir nodarīts kaitējums *ECRIS-TCN* sistēmai, attiecīgi minētā dalībvalsts, *Eurojust*, Eiropols vai *EPPO* ir atbildīga par šādu kaitējumu, izņemot gadījumu, kad un ciktāl *eu-LISA* vai cita dalībvalsts, kas piedalās *ECRIS-TCN* sistēmā, 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 atbildētājas dalībvalsts tiesību akti. Kompensācijas prasības, kuras vērstas pret *eu-LISA*, *Eurojust*, Eiropolu vai *EPPO* par kaitējumu, kas minēts 1. un 2. punktā, reglamentē to attiecīgie dibināšanas akti.

21. pants

Pašuzraudzība

Dalībvalstis nodrošina, ka katra centrālā iestāde veic vajadzīgos pasākumus, lai nodrošinātu atbilstību šai regulai, un vajadzības gadījumā sadarbojas ar uzraudzības iestādēm.

22. pants

Sankcijas

Jebkādai *ECRIS-TCN* sistēmā ievadīto datu ļaunprātīgai izmantošanai piemēro sankcijas vai disciplinārus pasākumus saskaņā ar valsts vai Savienības tiesību aktiem tā, lai sankcijas vai pasākumi būtu iedarbīgi, samērīgi un atturoši.

V NODAĻA

Tiesības uz datu aizsardzību un uzraudzība

23. pants

Datu pārzinis un datu apstrādātājs

1. Katra centrālā iestāde saskaņā ar piemērojamajiem Savienības datu aizsardzības noteikumiem ir uzskatāma par datu pārzini attiecībā uz persondatu apstrādi, ko attiecīgās centrālās iestādes dalībvalsts veic saskaņā ar šo regulu.

2. *eu-LISA* saskaņā ar Regulu (ES) 2018/1725 ir uzskatāma par datu apstrādātāju attiecībā uz persondatiem, ko dalībvalstis ievadījušas centrālajā sistēmā.

24. pants

Persondatu apstrādes mērķis

1. Centrālajā sistēmā iekļautos datus apstrādā tikai, lai identificētu dalībvalstis, kam ir sodāmības reģistra informācija par trešo valstu valstspiederīgajiem.

2. Piekļuve *ECRIS-TCN* sistēmai ir atļauta vienīgi pienācīgi pilnvarotiem centrālo iestāžu darbiniekiem, izņemot pienācīgi pilnvarotus *Eurojust*, Eiropola un *EPPO* darbiniekus, kuriem piekļuve *ECRIS-TCN* sistēmai ir noteikta šajā regulā. Piekļuve ir ierobežota tiktāl, ciktāl tas ir nepieciešams uzdevumu veikšanai saskaņā ar 1. punktā minēto mērķi un ciktāl tas ir nepieciešams un samērīgi ar izvirzītajiem mērķiem.

25. pants

Tiesības piekļūt, labot, dzēst un ierobežot apstrādi

1. Trešo valstu valstspiederīgo pieprasījumus, kas attiecas uz piemērojamos Savienības datu aizsardzības noteikumos izklāstītajām tiesībām piekļūt persondatiem, tos labot un dzēst, kā arī ierobežot persondatu apstrādi, var adresēt jebkuras dalībvalsts centrālajai iestādei.

2. Ja pieprasījums ir iesniegts dalībvalstij, kas nav notiesāšanas dalībvalsts, tā dalībvalsts, kurai pieprasījums iesniegts, bez liekas kavēšanās un jebkurā gadījumā 10 darba dienu laikā no pieprasījuma saņemšanas nosūta to notiesāšanas dalībvalstij. Pēc pieprasījuma saņemšanas notiesāšanas dalībvalsts:

a) nekavējoties sāk procedūru, lai pārbaudītu attiecīgo *ECRIS-TCN* sistēmā esošo datu precizitāti vai to apstrādes likumību; un

b) bez liekas kavēšanās atbild dalībvalstij, kas nosūtīja pieprasījumu.

3. Ja noskaidrojas, ka *ECRIS-TCN* sistēmā reģistrētie dati ir neprecīzi vai nelikumīgi apstrādāti, notiesāšanas dalībvalsts datus labo vai dzēš saskaņā ar 9. pantu. Notiesāšanas dalībvalsts vai attiecīgā gadījumā dalībvalsts, kurai ir iesniegts pieprasījums, bez liekas kavēšanās attiecīgajai personai rakstiski apstiprina to, ka ir veikti pasākumi, lai labotu vai dzēstu datus, kas attiecas uz šo personu. Notiesāšanas dalībvalsts bez liekas kavēšanās par veiktajiem pasākumiem informē arī ikvienu citu dalībvalsti, kas *ECRIS-TCN* sistēmā veiktas meklēšanas rezultātā saņēmusi informāciju par notiesājošiem spriedumiem.

4. Ja notiesāšanas dalībvalsts nepiekrīt tam, ka *ECRIS-TCN* sistēmā reģistrētie dati ir neprecīzi vai nelikumīgi apstrādāti, minētā dalībvalsts pieņem administratīvu vai tiesas lēmumu, kurā attiecīgajai personai rakstiski izskaidro, kāpēc tā nav gatava labot vai dzēst datus, kas attiecas uz šo personu. Attiecīgā gadījumā par šādiem gadījumiem var ziņot valsts uzraudzības iestādei.

5. Dalībvalsts, kas saskaņā ar 4. punktu pieņēmusi lēmumu, attiecīgajai personai sniedz arī informāciju, kurā paskaidrots, kādus pasākums minētā persona var veikt, ja tā nepiekrīt saskaņā ar 4. punktu sniegtajam paskaidrojumam. Tas ietver informāciju par to, kā iesniegt sūdzību vai celt prasību minētās dalībvalsts kompetentajās iestādēs vai tiesās, kā arī informāciju par palīdzību, tostarp no valsts uzraudzības iestādēm, kura ir pieejama saskaņā ar minētās dalībvalsts tiesību aktiem.

6. Visos pieprasījumos, kas iesniegti saskaņā ar 1. punktu, ir iekļauta informācija, kas vajadzīga, lai identificētu attiecīgo personu. Minēto informāciju izmanto vienīgi tam, lai varētu īstenot tiesības, kas minētas 1. punktā, un pēc tam to nekavējoties dzēš.

7. Ja ir piemērojams 2. punkts, centrālā iestāde, kurai tika adresēts pieprasījums, saglabā rakstisku uzskaiti par to, ka šāds pieprasījums ir veikts, kā tas ticis risināts un kurai iestādei tas ir pārsūtīts. Pēc valsts uzraudzības iestādes pieprasījuma centrālā iestāde nekavējoties dara minētajai valsts uzraudzības iestādei pieejamu attiecīgo uzskaiti. Centrālā iestāde un valsts uzraudzības iestāde dzēš šādas uzskaites trīs gadus pēc to izveidošanas.

26. pants

Sadarbība, lai nodrošinātu tiesību uz datu aizsardzību ievērošanu

1. Centrālās iestādes savstarpēji sadarbojas, lai nodrošinātu 25. pantā paredzēto tiesību ievērošanu.

2. Katrā dalībvalstī valsts uzraudzības iestāde pēc pieprasījuma sniedz ieinteresētajai personai informāciju par to, kā saskaņā ar piemērojamiem Savienības datu aizsardzības noteikumiem īstenot savas tiesības labot vai dzēst datus, kas uz šo personu attiecas.

3. Piemērojot šo pantu, tās dalībvalsts, kas pārsūtījusi datus, valsts uzraudzības iestāde un tās dalībvalsts valsts uzraudzības iestāde, kurai pieprasījums iesniegts, savstarpēji sadarbojas.

27. pants

Tiesiskās aizsardzības līdzekļi

Katrai personai saskaņā ar valsts vai Savienības tiesību aktiem ir tiesības iesniegt sūdzību un tiesības uz tiesiskās aizsardzības līdzekli notiesāšanas dalībvalstī, kura atteikusi 25. pantā minētās tiesības piekļūt datiem, kas uz viņu attiecas, vai tiesības labot vai dzēst šos datus.

28. pants

Valsts uzraudzības iestādes veiktā uzraudzība

1. Katra dalībvalsts nodrošina, ka valsts uzraudzības iestādes, kas izraudzītas, ievērojot piemērojamos Savienības datu aizsardzības noteikumus, uzrauga, vai ir likumīga 5. un 6. pantā minētā persondatu apstrāde, ko veic attiecīgā dalībvalsts, tostarp datu pārsūtīšana uz *ECRIS-TCN* sistēmu un no tās.

2. Valsts uzraudzības iestāde nodrošina, lai vismaz reizi trijos gados no *ECRIS-TCN* sistēmas darbības sākuma dienas tiktu veikta valsts sodāmības reģistros un pirkstu nospiedumu datubāzēs notikušo datu apstrādes darbību revīzija saistībā ar datu apmaiņu starp minētajām sistēmām un *ECRIS-TCN* sistēmu saskaņā ar attiecīgiem starptautiskiem revīzijas standartiem.

3. Dalībvalstis nodrošina to valsts uzraudzības iestādēm pietiekamus resursus tām saskaņā ar šo regulu uzticēto uzdevumu veikšanai.

4. Katra dalībvalsts sniedz jebkādu informāciju, ko pieprasījušas valsts uzraudzības iestādes, un jo īpaši tā sniedz minētajām iestādēm informāciju par darbībām, kas veiktas saskaņā ar 12., 13. un 19. pantu. Katra dalībvalsts piešķir valsts uzraudzības iestādēm piekļuvi tās reģistriem saskaņā ar 25. panta 7. punktu un ierakstiem saskaņā ar 31. panta 6. punktu, un ļauj tām jebkurā laikā piekļūt visām ar *ECRIS-TCN* sistēmu saistītajām telpām.

29. pants

Uzraudzība, ko veic Eiropas Datu aizsardzības uzraudzītājs

1. Eiropas Datu aizsardzības uzraudzītājs uzrauga, ka *eu-LISA* veiktā persondatu apstrāde saistībā ar *ECRIS-TCN* sistēmu notiek saskaņā ar šo regulu.

2. Eiropas Datu aizsardzības uzraudzītājs nodrošina, lai vismaz reizi trijos gados tiktu veikta *eu-LISA* veikto persondatu apstrādes darbību revīzija saskaņā ar attiecīgiem starptautiskiem revīzijas standartiem. Ziņojumu par minēto revīziju nosūta Eiropas Parlamentam, Padomei, Komisijai, *eu-LISA* un uzraudzības iestādēm. Pirms ziņojuma pieņemšanas *eu-LISA* dod iespēju izteikt piezīmes.

3. *eu-LISA* Eiropas Datu aizsardzības uzraudzītājam sniedz pieprasīto informāciju, nodrošina piekļuvi visiem dokumentiem un ierakstiem, kas minēti 31. pantā, kā arī nodrošina piekļuvi jebkurā laikā visām savām telpām.

30. pants

Sadarbība starp valsts uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju

Tiek nodrošināta saskaņota *ECRIS-TCN* sistēmas uzraudzība saskaņā ar Regulas (ES) 2018/1725 62. pantu.

31. pants

Ierakstu glabāšana

1. *eu-LISA* un kompetentās iestādes saskaņā ar to attiecīgajām atbildības jomām nodrošina, ka visas datu apstrādes darbības *ECRIS-TCN* sistēmā tiek ierakstītas saskaņā ar 2. punktu, lai varētu pārbaudīt, vai pieprasījumi atbilst nosacījumiem, uzraudzīt datu integritāti un drošību un datu apstrādes likumību, kā arī lai varētu veikt pašuzraudzību.

2. Ierakstā tiek sniegta šāda informācija:

a) pieprasījuma par piekļuvi *ECRIS-TCN* sistēmas datiem mērķis;

b) šīs regulas 5. pantā minētie pārsūtītie dati;

c) valsts lietas numurs;

d) darbības datums un precīzs laiks;

e) meklēšanā izmantotie dati;

f) tās amatpersonas pazīšanas zīme, kas veica meklēšanu.

3. Ieraksts par aplūkotajiem datiem un atklāto informāciju dod iespēju noteikt šādu darbību pamatojumu.

4. Ierakstus izmanto tikai, lai uzraudzītu datu apstrādes likumību un lai nodrošinātu datu integritāti un drošību. Šīs regulas 36. pantā minētajai uzraudzībai un novērtēšanai var izmantot tikai ierakstus, kas neietver persondatus. Minētos ierakstus aizsargā ar piemērotiem pasākumiem pret neatļautu piekļuvi, un tos dzēš pēc trim gadiem, ja tie vairs nav vajadzīgi jau sāktām uzraudzības procedūrām.

5. *eu-LISA* pēc pieprasījuma un bez liekas kavēšanās centrālajām iestādēm dara pieejamus ierakstus par savām apstrādes darbībām.

6. Kompetentajām valsts uzraudzības iestādēm, kuras ir atbildīgas par to, lai pārbaudītu, vai pieprasījums atbilst nosacījumiem, un uzraudzītu datu apstrādes likumību un datu integritāti un drošību, pēc to pieprasījuma nodrošina piekļuvi ierakstiem, lai tās varētu veikt savus uzdevumus. Centrālās iestādes pēc pieprasījuma un bez liekas kavēšanās kompetentajām valsts uzraudzības iestādēm dara pieejamus ierakstus par savām apstrādes darbībām.

VI NODAĻA

Nobeiguma noteikumi

32. pants

Datu izmantošana pārskatiem un statistikai

1. Pienācīgi pilnvarotiem *eu-LISA*, kompetento iestāžu un Komisijas darbiniekiem ir piekļuve *ECRIS-TCN* sistēmā apstrādātiem datiem tikai ziņošanas un statistikas nolūkos bez iespējas veikt individuālu identificēšanu.

2. Šā panta 1. punkta nolūkā *eu-LISA* savos tehniskajos birojos ievieš, īsteno un mitina centrālo repozitoriju, kurā glabā šā panta 1. punktā minētos datus, kas bez iespējas veikt individuālu identificēšanu, ļauj iegūt pielāgojamus ziņojumus un statistiku. Piekļuvi centrālajam repozitorijam piešķir, izmantojot drošu piekļuvi ar piekļuves kontroli un īpašiem lietotāju profiliem tikai pārskatu un statistikas vajadzībām.

3. Procedūras, kuras *eu-LISA* ieviesusi, lai uzraudzītu *ECRIS-TCN* sistēmas darbību, kā minēts 36. pantā, kā arī *ECRIS* ieteicamo īstenošanas programmatūru, ietver iespēju sagatavot regulārus statistikas datus uzraudzības vajadzībām.

Katru mēnesi *eu-LISA* iesniedz Komisijai statistiku par no sodāmības reģistriem iegūtas informācijas ierakstīšanu, glabāšanu un apmaiņu, izmantojot *ECRIS-TCN* sistēmu un *ECRIS* ieteicamo īstenošanas programmatūru. *eu-LISA* nodrošina, ka, izmantojot minēto statistiku, nav iespējams veikt individuālu identificēšanu. Pēc Komisijas pieprasījuma *eu-LISA* sniedz tai statistikas datus par konkrētiem aspektiem, kas saistīti ar šīs regulas īstenošanu.

4. Dalībvalstis *eu-LISA* sniedz statistikas datus, kas vajadzīgi šajā pantā minēto pienākumu veikšanai. Tās Komisijai sniedz statistikas datus par notiesāto trešo valstu valstspiederīgo skaitu, kā arī par attiecībā uz trešo valstu valstspiederīgajiem pieņemtu notiesājošu spriedumu skaitu to teritorijā.

33. pants

Izmaksas

1. Izmaksas, kas saistītas ar centrālās sistēmas, 4. panta 1. punkta d) apakšpunktā minētās komunikācijas infrastruktūras, saskarnes programmatūras un *ECRIS* ieteicamās īstenošanas programmatūras izveidi un darbību, sedz no Savienības vispārējā budžeta.

2. Izmaksas, kas saistītas ar *Eurojust*, Eiropola un *EPPO* pievienošanu *ECRIS-TCN* sistēmai, sedz no to attiecīgajiem budžetiem.

3. Citas izmaksas sedz dalībvalstis, jo īpaši izmaksas, kas radušās saistībā ar esošo valsts sodāmības reģistru, pirkstu nospiedumu datubāzu un centrālo iestāžu pievienošanu *ECRIS-TCN* sistēmai, kā arī izmaksas, kas saistītas ar *ECRIS* ieteicamās īstenošanas programmatūras mitināšanu.

34. pants

Paziņojumi

1. Katra dalībvalsts paziņo *eu-LISA* par savu centrālo iestādi, kurai ir piekļuve datu ievadīšanai, labošanai, dzēšanai, aplūkošanai vai meklēšanai, kā arī par jebkādām izmaiņām šajā sakarā.

2. *eu-LISA* nodrošina, ka dalībvalstu paziņoto centrālo iestāžu saraksts tiek publicēts gan *Eiropas Savienības Oficiālajā Vēstnesī*, gan tās tīmekļa vietnē. Ja *eu-LISA* saņem paziņojumu par izmaiņām dalībvalsts centrālajā iestādē, tā bez liekas kavēšanās sarakstu atjaunina.

35. pants

Datu ievadīšana un darbības sākums

1. Kad Komisija ir pārliecinājusies, ka ir izpildīti turpmāk minētie nosacījumi, tā nosaka datumu, no kura dalībvalstis *ECRIS-TCN* sistēmā sāk ievadīt 5. pantā minētos datus:

a) ir pieņemti 10. pantā minētie attiecīgie īstenošanas akti;

b) dalībvalstis ir validējušas tehnisko un juridisko kārtību, lai 5. pantā minētos datus vāktu un pārsūtītu uz *ECRIS-TCN* sistēmu, un par minēto kārtību ir paziņojušas Komisijai;

c) *eu-LISA* sadarbībā ar dalībvalstīm, izmantojot anonīmus testa datus, ir veikusi visaptverošu *ECRIS-TCN* sistēmas testu.

2. Kad Komisija saskaņā ar 1. punktu ir noteikusi datumu, kurā var sākt ievadīt datus, tā šo datumu paziņo dalībvalstīm. Divu mēnešu laikā pēc minētā datuma dalībvalstis ievada 5. pantā minētos datus *ECRIS-TCN* sistēmā, ņemot vērā 41. panta 2. punktu.

3. Pēc 2. punktā minētā laikposma beigām *eu-LISA* sadarbībā ar dalībvalstīm veic *ECRIS-TCN* sistēmas galīgo testu.

4. Kad 3. punktā minētais tests ir sekmīgi pabeigts, un *eu-LISA* uzskata, ka *ECRIS-TCN* sistēma ir gatava sākt darboties, tā par to paziņo Komisijai. Komisija par testa rezultātiem paziņo Eiropas Parlamentam un Padomei un pieņem lēmumu par datumu, no kura *ECRIS-TCN* sistēmai jāsāk darboties.

5. Komisijas lēmumu par *ECRIS-TCN* sistēmas darbības sākuma datumu, kā minēts 4. punktā, publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

6. Dalībvalstis sāk izmantot *ECRIS-TCN* sistēmu no dienas, ko Komisija noteikusi saskaņā ar 4. punktu.

7. Pieņemot šajā pantā minētos lēmumus, Komisija var noteikt atšķirīgus datumus, kad *ECRIS-TCN* sistēmā ievadīt burtciparu datus un pirkstu nospiedumu datus, kā minēts 5. pantā, kā arī to, kad sākt darbības attiecībā uz šo datu dažādajām kategorijām.

36. pants

Uzraudzība un izvērtēšana

1. *eu-LISA* nodrošina, ka ir ieviestas procedūras, lai uzraudzītu *ECRIS-TCN* sistēmas izstrādi, ņemot vērā ar plānošanu un izmaksām saistītos mērķus, un lai uzraudzītu *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras darbību, ņemot vērā ar pakalpojuma tehniskajiem rezultātiem, rentabilitāti, drošību un kvalitāti saistītos mērķus.

2. Lai pārraudzītu *ECRIS-TCN* sistēmas darbību un tās tehnisko apkopi, *eu-LISA* ir piekļuve vajadzīgajai informācijai, kas attiecas uz datu apstrādes darbībām, kuras veiktas *ECRIS-TCN* sistēmā un *ECRIS* ieteicamajā īstenošanas programmatūrā.

3. Līdz 2019. gada 12. decembrim un turpmāk ik pēc sešiem mēnešiem plānošanas un izstrādes posma laikā *eu-LISA* iesniedz ziņojumu Eiropas Parlamentam un Padomei par aktuālo situāciju saistībā ar *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras izstrādi.

4. 3. punktā minētajā ziņojumā iekļauj pārskatu par pašreizējām izmaksām un par projekta progresu, finansiālās ietekmes novērtējumu, kā arī informāciju par jebkādām tehniskām problēmām un riskiem, kas var ietekmēt *ECRIS-TCN* sistēmas kopējās izmaksas, kuras sedzamas no Savienības vispārējā budžeta saskaņā ar 33. pantu.

5. Ja izstrādes process ievērojami kavējas, *eu-LISA* pēc iespējas drīz informē Eiropas Parlamentu un Padomi par šīs kavēšanās iemesliem, kā arī par tās ietekmi laika un finanšu ziņā.

6. Tiklīdz *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras izstrāde ir pabeigta, *eu-LISA* iesniedz Eiropas Parlamentam un Padomei ziņojumu, kurā izskaidrots, kā tika sasniegti mērķi, jo īpaši saistībā ar plānošanu un izmaksām, un pamatotas jebkādas novirzes.

7. *ECRIS-TCN* sistēmas tehniskās atjauninašanas gadījumā, kas varētu radīt būtiskas izmaksas, *eu-LISA* par to informē Eiropas Parlamentu un Padomi.

8. Divus gadus pēc *ECRIS-TCN* sistēmas darbības sākuma un turpmāk ik gadu *eu-LISA* iesniedz Komisijai ziņojumu par *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras tehnisko darbību, tostarp attiecībā uz to drošību, jo īpaši pamatojoties uz statistikas datiem par *ECRIS-TCN* sistēmas darbību un izmantošanu un no sodāmības reģistriem iegūtas informācijas apmaiņu, izmantojot *ECRIS* ieteicamās īstenošanas programmatūru.

9. Četrus gadus pēc *ECRIS-TCN* sistēmas darbības sākuma un turpmāk ik pēc četriem gadiem Komisija veic *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras vispārēju novērtējumu. Uz šā pamata sagatavotajā vispārējā novērtējuma ziņojumā ietver šīs regulas piemērošanas izvērtējumu un analīzi par sasniegtajiem rezultātiem, tos salīdzinot ar izvirzītajiem mērķiem, un par ietekmi uz pamattiesībām. Ziņojumā ietver arī izvērtējumu par to, vai *ECRIS-TCN* sistēmas darbības pamatojums vēl joprojām ir spēkā, izvērtējumu par *ECRIS-TCN* sistēmas nolūkos izmantoto biometrisko datu piemērotību, izvērtējumu par *ECRIS-TCN* sistēmas drošību un par jebkādu drošības ietekmi uz turpmākajām darbībām. Novērtējumā iekļauj visus vajadzīgos ieteikumus. Komisija ziņojumu nosūta Eiropas Parlamentam, Padomei, Eiropas Datu aizsardzības uzraudzītājam un Eiropas Savienības Pamattiesību aģentūrai.

10. Turklāt 9. punktā minētajā pirmajā vispārējā novērtējumā izvērtē:

a) pamatojoties uz attiecīgiem statistikas datiem un sīkāku informāciju no dalībvalstīm, to, cik lielā mērā šīs regulas mērķu sasniegšanu ir sekmējusi *ECRIS-TCN* sistēmā iekļauta identitātes informācija par Savienības pilsoņiem, kuriem ir arī trešās valsts valstspiederība;

b) vai dažām dalībvalstīm ir iespēja turpināt izmantot 4. pantā minēto valsts *ECRIS* īstenošanas programmatūru;

c) pirkstu nospiedumu datu ievadīšanu *ECRIS-TCN* sistēmā, jo īpaši 5. panta 1. punkta b) apakšpunkta ii) punktā minēto minimālo kritēriju piemērošanu;

d) *ECRIS* un *ECRIS-TCN* sistēmas ietekmi uz persondatu aizsardzību.

Izvērtējumam vajadzības gadījumā var pievienot tiesību aktu priekšlikumus. Turpmākajos vispārējos novērtējumos var iekļaut jebkura vai visu šo aspektu izvērtējumu.

11. Dalībvalstis, *Eurojust*, Eiropols un *EPPO* saskaņā ar kvantitatīvajiem rādītājiem, kurus iepriekš noteikusi Komisija un/vai *eu-LISA*, sniedz *eu-LISA* un Komisijai informāciju, kas vajadzīga, lai izstrādātu 3., 8. un 9. punktā minētos ziņojumus. Šī informācija neapdraud darba metodes, un tajā nav ietverta informācija, kas atklāj avotus, darbiniekus vai izmeklēšanas.

12. Attiecīgā gadījumā uzraudzības iestādes saskaņā ar kvantitatīvajiem rādītājiem, kurus iepriekš noteikusi Komisija vai *eu-LISA* vai abi, sniedz *eu-LISA* un Komisijai informāciju, kas vajadzīga, lai izstrādātu 9. punktā minētos ziņojumus. Šī informācija neapdraud darba metodes, un tajā nav ietverta informācija, kas atklāj avotus, darbiniekus vai izmeklēšanas.

13. *eu-LISA* sniedz Komisijai informāciju, kas vajadzīga, lai izstrādātu 9. punktā minētos vispārējos novērtējumus.

37. pants

Deleģēšanas īstenošana

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

2. Pilnvaras pieņemt 6. panta 2. punktā minētos deleģētos aktus Komisijai piešķir uz nenoteiktu laiku no 2019. gada 11. jūnija.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 6. panta 2. 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 6. panta 2. 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.

38. 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.

Ja komiteja nesniedz atzinumu, Komisija nepieņem īstenošanas akta projektu, un piemēro Regulas (ES) Nr. 182/2011 5. panta 4. punkta trešo daļu.

39. pants

Padomdevēja grupa

eu-LISA izveido padomdevēju grupu, lai iegūtu zinātību, kas saistīta ar *ECRIS-TCN* sistēmu un *ECRIS* ieteicamo īstenošanas programmatūru, īpaši attiecībā uz gada darba programmas un gada darbības pārskata sagatavošanu. Plānošanas un izstrādes posmā piemēro 11. panta 9. punktu.

40. pants

Grozījumi Regulā (ES) 2018/1726

Regulu (ES) 2018/1726 groza šādi:

1) regulas 1. panta 4. punktu aizstāj ar šādu:

"4. Aģentūra ir atbildīga par ieceļošanas/izceļošanas sistēmas (IIS), *DubliNet* un Eiropas ceļošanas informācijas un atļauju sistēmas (*ETIAS*) *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras sagatavošanu, izstrādi un/vai darbības pārvaldību.";

2) iekļauj šādu pantu:

"*8.a pants*

Ar *ECRIS-TCN* sistēmu un *ECRIS* ieteicamās īstenošanas programmatūru saistītie uzdevumi

Attiecībā uz *ECRIS-TCN* sistēmu un *ECRIS* ieteicamo īstenošanas programmatūru aģentūra veic:

a) uzdevumus, kas tai uzticēti saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/816 (*);

b) uzdevumus, kas saistīti ar mācībām par *ECRIS-TCN* sistēmu un *ECRIS* ieteicamās īstenošanas programmatūras tehnisko izmantojumu.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/816 (2019. gada 17. aprīlis), ar ko Eiropas Sodāmības reģistru informācijas sistēmas papildināšanai izveido centralizētu sistēmu (*ECRIS-TCN* sistēma) tādu dalībvalstu identificēšanai, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un ar ko groza Regulu (ES) 2018/1726 (OV L 135, 22.5.2019., 1. lpp.).";

3) regulas 14. panta 1. punktu aizstāj ar šādu:

"1. Izpētes jomā aģentūra pārrauga norises, kuras skar *SIS II*, VIS, *Eurodac*, IIS, *ETIAS*, *DubliNet*, *ECRIS-TCN* sistēmas un citu 1. panta 5. punktā minēto lielapjoma IT sistēmu darbības pārvaldību.";

4) regulas 19. panta 1. punktu groza šādi:

a) punkta ee) apakšpunktu aizstāj ar šādu:

"ee) pieņem ziņojumus par IIS izstrādi saskaņā ar Regulas (ES) 2017/2226 72. panta 2. punktu, ziņojumus par *ETIAS* izstrādi saskaņā ar Regulas (ES) 2018/1240 92. panta 2. punktu un ziņojumus par *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras izstrādi saskaņā ar Regulas (ES) 2019/816 36. panta 3. punktu;";

b) punkta ff) apakšpunktu aizstāj ar šādu:

"ff) pieņem ziņojumus par *SIS II* tehnisko darbību saskaņā ar attiecīgi Regulas (EK) Nr. 1987/2006 50. panta 4. punktu un Lēmuma 2007/533/TI 66. panta 4. punktu, par VIS tehnisko darbību saskaņā ar Regulas (EK) Nr. 767/2008 50. panta 3. punktu un Lēmuma 2008/633/TI 17. panta 3. punktu, par IIS tehnisko darbību saskaņā ar Regulas (ES) 2017/2226 72. panta 4. punktu, *ETIAS* saskaņā ar Regulas (ES) 2018/1240 92. panta 4. punktu un par *ECRIS-TCN* sistēmas un *ECRIS* ieteicamās īstenošanas programmatūras tehnisko darbību saskaņā ar Regulas (ES) 2019/816 36. panta 8. punktu;";

c) punkta hh) apakšpunktu aizstāj ar šādu:

"hh) pieņem oficiālus komentārus par Eiropas Datu aizsardzības uzraudzītāja ziņojumiem par revīzijām, kas veiktas saskaņā ar Regulas (EK) Nr. 1987/2006 45. panta 2. punktu, Regulas (EK) Nr. 767/2008 42. panta 2. punktu un Regulas (ES) Nr. 603/2013 31. panta 2. punktu, Regulas (ES) 2017/2226 56. panta 2. punktu, Regulas (ES) 2018/1240 67. pantu un Regulas (ES) 2019/816 29. panta 2. punktu, un nodrošina atbilstošus pēcpasākumus pēc šīm revīzijām;";

d) iekļauj šādu apakšpunktu:

"lla) iesniedz Komisijai statistiku saistībā ar *ECRIS-TCN* sistēmu un *ECRIS* ieteicamo īstenošanas programmatūru saskaņā ar Regulas (ES) 2019/816 32. panta 4. punkta otro daļu;";

e) punkta mm) apakšpunktu aizstāj ar šādu:

"mm) nodrošina, ka ik gadu publicē tādu kompetentu iestāžu sarakstu, kas ir pilnvarotas veikt *SIS II* iekļauto datu tiešu meklēšanu saskaņā ar Regulas (EK) Nr. 1987/2006 31. panta 8. punktu un Lēmuma 2007/533/TI 46. panta 8. punktu, kā arī *SIS II* valstu sistēmu biroju (*N.SIS II* biroji) un *SIRENE* biroju sarakstu, kā minēts attiecīgi Regulas (EK) Nr. 1987/2006 7. panta 3. punktā un Lēmuma 2007/533/TI 7. panta 3. punktā, kā arī kompetento iestāžu sarakstu saskaņā ar Regulas (ES) 2017/2226 65. panta 2. punktu, kompetento iestāžu sarakstu saskaņā ar Regulas (ES) 2018/1240 87. panta 2. punktu un centrālo iestāžu sarakstu saskaņā ar Regulas (ES) 2019/816 34. panta 2. punktu;";

5) regulas 22. panta 4. punktā aiz trešās daļas iekļauj šādu daļu:

"*Eurojust*, Eiropols un *EPPO* var piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par *ECRIS-TCN* sistēmu attiecībā uz Regulas (ES) 2019/816 piemērošanu.";

6) regulas 24. panta 3. punkta p) apakšpunktu aizstāj ar šādu:

"p) to, lai, neskarot Civildienesta noteikumu 17. pantu, tiktu noteiktas konfidencialitātes prasības ar mērķi panākt atbilstību Regulas (EK) Nr. 1987/2006 17. pantam, Lēmuma 2007/533/TI 17. pantam, Regulas (EK) Nr. 767/2008 26. panta 9. punktam, Regulas (ES) Nr. 603/2013 4. panta 4. punktam, Regulas (ES) 2017/2226 37. panta 4. punktam, Regulas (ES) 2018/1240 74. panta 2. punktam un Regulas (ES) 2019/816 11. panta 16. punktam;";

7) regulas 27. panta 1. punktā iekļauj šādu punktu:

"da) *ECRIS-TCN* sistēmas padomdevēju grupa;".

41. pants

Īstenošana un pārejas noteikumi

1. Dalībvalstis, cik drīz vien iespējams, veic vajadzīgos pasākumus šīs regulas prasību izpildei, lai nodrošinātu *ECRIS-TCN* sistēmas pienācīgu darbību.

2. Attiecībā uz notiesājošiem spriedumiem, kas pieņemti pirms datu ievadīšanas sākuma datuma saskaņā ar 35. panta 1. punktu, centrālās iestādes izveido atsevišķus datu ierakstus centrālajā sistēmā, ņemot vērā, ka:

a) burtciparu datus centrālajā sistēmā ievada līdz 35. panta 2. punktā minētā laikposma beigām;

b) pirkstu nospiedumu datus centrālajā sistēmā ievada vēlākais divu gadu laikā pēc darbības sākuma saskaņā ar 35. panta 4. punktu.

42. pants

Stāšanās spēkā

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

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

Strasbūrā, 2019. gada 17. aprīlī

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*
A. TAJANI	G. CIAMBA

PIELIKUMS

REGULAS (ES) 2019/816 17. PANTA 1. PUNKTĀ MINĒTĀ INFORMĀCIJAS PIEPRASĪJUMA STANDARTVEIDLAPA INFORMĀCIJAS IEGŪŠANAI PAR DALĪBVALSTI, KURAI VARĒTU BŪT SODĀMĪBAS REĢISTRA INFORMĀCIJA PAR TREŠĀS VALSTS VALSTSPIEDERĪGO

Šī veidlapa, kura visās 24 Savienības iestāžu oficiālajās valodās ir pieejama vietnē www.eurojust.europa.eu, būtu jānosūta uz e-pasta adresi ECRIS-TCN@Eurojust.europa.eu vienā no minētajām valodām.

Pieprasījuma iesniedzēja valsts vai starptautiska organizācija:

Valsts vai starptautiskās organizācijas nosaukums:
Pieprasījuma iesniedzēja iestāde:
Persona, kas to pārstāv *(personas vārds, uzvārds)*:
Amats:
Adrese:
Tālruņa numurs:
E-pasta adrese:

Kriminālprocess, par kuru tiek pieprasīta informācija:

Iekšējais atsauces numurs:
Kompetentā iestāde:
Izmeklējamo noziegumu veids *(lūgums minēt krimināLkodeksa attiecīgo(-os) pantu(-us))*:
Cita attiecīga informācija *(piemēram, pieprasījuma steidzamība)*:

Identitātes informācija par personu, kurai ir kādas trešās valsts valstspiederība un attiecībā uz kuru tiek pieprasīta informācija par notiesāšanas dalībvalsti:

NB: lūgums sniegt pēc iespējas plašāku informāciju.

Uzvārds:
Vārds(-i):
Dzimšanas datums:
Dzimšanas vieta *(pilsēta un valsts)*:
Valstspiederība vai valstspiederības:
Dzimums:
Iepriekšējais(-ie) vārds(-i), ja tāds(-i) ir:
Vecāku vārdi un uzvārdi:
Identitātes numurs:
Personas identifikācijas dokumenta(-u) veids un numurs:
Dokumenta(-u) izdevējiestāde:
Pseidonīmi vai pieņemtie vārdi:
Ja ir pieejami pirkstu nospiedumu dati, lūgums tos iesniegt.

Vairāku personu gadījumā lūgums norādīt tās atsevišķi.

Nolaižamā izvēlne dotu iespēju iekļaut papildu personas

Vieta	
Datums	

(Elektroniskais) paraksts un zīmogs:

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2019/817

(2019. gada 20. maijs),

ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16. panta 2. punktu, 74. pantu un 77. panta 2. punkta a), b), d) un e) apakšpunktu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu ([1]),

pēc apspriešanās ar Reģionu komiteju,

saskaņā ar parasto likumdošanas procedūru ([2]),

tā kā:

(1) Komisija 2016. gada 6. aprīļa paziņojumā "Spēcīgākas un viedākas robežu un drošības informācijas sistēmas" uzsvēra nepieciešamību uzlabot Savienības datu pārvaldības arhitektūru robežu pārvaldības un drošības jomā. Ar šo paziņojumu tika sākta virzība uz ES drošības, robežu un migrācijas pārvaldības informācijas sistēmu sadarbspējas panākšanu, lai novērstu ar šīm sistēmām saistītos strukturālos trūkumus, kas apgrūtina valsts iestāžu darbu, un nodrošinātu, ka robežsargu, muitas iestāžu, policijas darbinieku un tiesu iestāžu rīcībā ir nepieciešamā informācija.

(2) 2016. gada 6. jūnija Ceļvedī ar mērķi uzlabot informācijas apmaiņu un informācijas pārvaldību, tostarp sadarbspējas risinājumus, tieslietu un iekšlietu jomā Padome apzināja dažādas tiesiskas, tehniskas un operatīvas problēmas ES informācijas sistēmu sadarbspējā un aicināja rast atbilstošus risinājumus.

(3) 2016. gada 6. jūlija rezolūcijā par stratēģiskajām prioritātēm attiecībā uz Komisijas 2017. gada darba programmu ([3]) Eiropas Parlaments aicināja iesniegt priekšlikumus par pastāvošo informācijas sistēmu uzlabošanu un attīstīšanu, informācijas trūkumu novēršanu un šo sistēmu sadarbspējas panākšanu, kā arī priekšlikumus par obligāto informācijas apmaiņu ES, kuri papildināti ar nepieciešamajiem mehānismiem datu aizsardzībai.

(4) Eiropadome savos 2016. gada 15. decembra secinājumos aicināja turpināt darbu, lai izveidotu ES informācijas sistēmu un datubāzu sadarbspēju.

(5) Augsta līmeņa ekspertu grupa informācijas sistēmu un sadarbspējas jautājumos 2017. gada 11. maija galīgajā ziņojumā secināja, ka ir nepieciešams un tehniski iespējams sākt darbu pie praktiskiem sadarbspējas risinājumiem un ka sadarbspēja principā var gan sniegt operatīvos ieguvumus, gan to var izstrādāt atbilstīgi datu aizsardzības prasībām.

([1]) OV C 283, 10.8.2018., 48. lpp.
([2]) Eiropas Parlamenta 2019. gada 16. aprīļa nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2019. gada 14. maija lēmums.
([3]) OV C 101, 16.3.2018., 116. lpp.

(6) 2017. gada 16. maija paziņojumā "Septītais progresa ziņojums virzībā uz efektīvu un patiesu drošības savienību" Komisija – saskaņā ar 2016. gada 6. aprīļa paziņojumu un ņemot vērā konstatējumus un ieteikumus, kurus izteikusi augsta līmeņa ekspertu grupa informācijas sistēmu un sadarbspējas jautājumos, – izklāstīja jaunu pieeju robežu, drošības un migrācijas datu pārvaldībai, saskaņā ar kuru visām ES informācijas sistēmām drošības, robežu un migrācijas pārvaldības jomā jābūt sadarbspējīgām, pilnībā ievērojot pamattiesības.

(7) 2017. gada 9. jūnija secinājumos par turpmāko virzību ar mērķi uzlabot informācijas apmaiņu un nodrošināt ES informācijas sistēmu sadarbspēju Padome aicināja Komisiju rast sadarbspējas risinājumus, kā ierosinājusi augsta līmeņa ekspertu grupa.

(8) Eiropadome savos 2017. gada 23. jūnija secinājumos uzsvēra nepieciešamību uzlabot sadarbspēju starp datubāzēm un aicināja Komisiju cik drīz vien iespējams sagatavot tiesību akta projektu, pamatojoties uz priekšlikumiem, kurus izteikusi augsta līmeņa ekspertu grupa informācijas sistēmu un sadarbspējas jautājumos.

(9) Lai uzlabotu pārbaužu lietderību un efektivitāti pie ārējām robežām, palīdzētu novērst un apkarot nelikumīgu imigrāciju un sekmētu augsta drošības līmeņa nodrošināšanu Savienības brīvības, drošības un tiesiskuma telpā, tostarp uzturot sabiedrisko drošību un sabiedrisko kārtību un sargājot drošību dalībvalstu teritorijās, uzlabotu kopējās vīzu politikas īstenošanu, palīdzētu starptautiskās aizsardzības pieteikumu izskatīšanā, palīdzētu novērst, atklāt un izmeklēt teroristu nodarījumus un citus smagus noziedzīgus nodarījumus, palīdzētu identificēt nezināmas personas, kuras nespēj sevi identificēt, vai neidentificētas mirstīgās atliekas dabas katastrofas, negadījuma vai teroristu uzbrukuma gadījumā, lai saglabātu sabiedrības uzticēšanos Savienības migrācijas un patvēruma sistēmai, Savienības drošības pasākumiem un Savienības spējām pārvaldīt ārējo robežu, būtu jāizveido sadarbspēja starp ES informācijas sistēmām, proti, ieceļošanas/izceļošanas sistēmu (IIS), vīzu informācijas sistēmu (VIS), Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*), *Eurodac*, Šengenas informācijas sistēmu (*SIS*) un Eiropas Sodāmības reģistru informācijas sistēmu trešo valstu valstspiederīgajiem (*ECRIS-TCN*), lai šīs ES informācijas sistēmas un to dati papildinātu cita citu, vienlaikus ievērojot personas pamattiesības, jo īpaši tiesības uz personas datu aizsardzību. Lai to panāktu, kā sadarbspējas komponenti būtu jāizveido Eiropas meklēšanas portāls (*ESP*), kopējs biometrisko datu salīdzināšanas pakalpojums (kopējais *BMS*), kopējs identitātes repozitorijs (*CIR*) un vairāku identitāšu detektors (*MID*).

(10) ES informācijas sistēmu sadarbspējai būtu jāļauj tām papildināt citai citu, lai atvieglotu personu, tostarp personu, kuras nespēj sevi identificēt, vai neidentificētu cilvēku mirstīgo atlieku, pareizu identifikāciju, palīdzētu apkarot identitātes viltošanu, uzlabotu un saskaņotu attiecīgo ES informācijas sistēmu prasības datu kvalitātes jomā, atvieglotu dalībvalstīm ES informācijas sistēmu tehnisko un operatīvo īstenošanu, pastiprinātu attiecīgajām ES informācijas sistēmām piemērojamos datu drošības un datu aizsardzības pasākumus, racionalizētu piekļuvi IIS, VIS, *ETIAS* un *Eurodac* nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus un atbalstītu IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

(11) Sadarbspējas komponentiem būtu jāaptver IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN*. Tiem būtu jāaptver arī Eiropola dati, bet vienīgi tiktāl, lai Eiropola datos varētu veikt vaicājumus vienlaikus ar minētajām ES informācijas sistēmām.

(12) Sadarbspējas komponentiem būtu jāapstrādā tādu personu personas dati, kuru personas dati tiek apstrādāti pamatā esošajās ES informācijas sistēmās un Eiropolā.

(13) Būtu jāizveido *ESP*, lai tehniski sekmētu dalībvalstu iestāžu un Savienības aģentūru ātru, netraucētu, efektīvu, sistemātisku un kontrolētu piekļuvi ES informācijas sistēmām, Eiropola datiem un Starptautiskās Kriminālpolicijas organizācijas (Interpola) datubāzēm, ciktāl tas vajadzīgs to uzdevumu izpildei un saskaņā ar to piekļuves tiesībām. *ESP* arī būtu jāatbalsta IIS, VIS, *ETIAS*, *Eurodac*, *SIS*, *ECRIS-TCN* un Eiropola datu mērķi. Nodrošinot iespēju paralēli veikt vaicājumus visās attiecīgajās ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs, *ESP*

būtu jādarbojas kā vienloga sistēmai jeb "ziņojumu starpniekam", lai meklētu datus dažādās centrālajās sistēmās un netraucēti izgūtu vajadzīgo informāciju, pilnībā ievērojot pamatā esošo sistēmu prasības attiecībā uz piekļuves kontroli un datu aizsardzību.

(14) *ESP* uzbūvei būtu jānodrošina, ka dati, ko *ESP* lietotājs izmanto vaicājuma veikšanai Interpola datubāzēs, netiek atklāti Interpola datu īpašniekiem. *ESP* uzbūvei būtu arī jānodrošina, lai vaicājumi Interpola datubāzē tiktu veikti vienīgi saskaņā ar piemērojamiem Savienības un valsts tiesību aktiem.

(15) Interpola Zagto un pazaudēto ceļošanas dokumentu datubāze (*SLTD* datubāze) ļauj pilnvarotām struktūrām, kas atbildīgas par teroristu nodarījumu un citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu vai izmeklēšanu dalībvalstīs, tostarp imigrācijas un robežkontroles iestādēm, noteikt ceļošanas dokumenta derīgumu. Izmantojot *ETIAS*, tiek veikti vaicājumi *SLTD* datubāzē un Interpola datubāzē ar ceļošanas dokumentiem, par kuriem izdoti paziņojumi (*TDAWN* datubāze), lai novērtētu, vai persona, kas iesniedz ceļošanas atļaujas pieteikumu, varētu, piemēram, neatbilstīgi migrēt vai radīt drošības apdraudējumu. *ESP* būtu jānodrošina iespēja veikt vaicājumus *SLTD* un *TDAWN* datubāzēs, izmantojot personas identitātes datus vai ceļošanas dokumenta datus. Gadījumos, kad personas datus no Savienības nosūta Interpolam, izmantojot *ESP*, būtu jāpiemēro noteikumi par starptautisku nosūtīšanu, kas paredzēti Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 ([4]) V nodaļā, vai valsts noteikumi, ar kuriem transponē Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680 ([5]) V nodaļu. Tam nebūtu jāskar īpašie noteikumi, kas paredzēti Padomes Kopējā nostājā 2005/69/TI ([6]) un Padomes Lēmumā 2007/533/TI ([7]).

(16) *ESP* būtu jāizstrādā un jākonfigurē tā, lai tas ļautu veikt vaicājumus, vienīgi izmantojot datus, kas saistīti ar personām vai ceļošanas dokumentiem, kuri ir ietverti kādā ES informācijas sistēmā, Eiropola datos vai Interpola datubāzēs.

(17) Lai nodrošinātu attiecīgo ES informācijas sistēmu sistemātisku izmantošanu, *ESP* būtu jāizmanto, lai veiktu vaicājumus *CIR*, IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN*. Tomēr būtu jāsaglabā valsts pieslēgums dažādajām ES informācijas sistēmām, lai nodrošinātu tehnisku rezerves mehānismu. Arī Savienības aģentūrām būtu jāizmanto *ESP*, lai savu uzdevumu izpildes nolūkā veiktu vaicājumus centrālajā *SIS* saskaņā ar savām piekļuves tiesībām. *ESP* vajadzētu būt papildu līdzeklim, ar ko veikt vaicājumus centrālajā *SIS*, Eiropola datos un Interpola datubāzēs, papildinot esošās specializētās saskarnes.

(18) Biometriskie dati, piemēram, pirkstu nospiedumi un sejas attēli, ir unikāli un tādēļ personas identifikācijai daudz ticamāki nekā burtciparu dati. Kopējam *BMS* vajadzētu būt tehniskam rīkam, kas pastiprina un atvieglo attiecīgo ES informācijas sistēmu un pārējo sadarbspējas komponentu darbu. Kopējā *BMS* galvenajam mērķim vajadzētu būt atvieglot vairākās datubāzēs reģistrētas personas identifikāciju, izmantojot vienu tehnoloģisko komponentu, lai salīdzinātu minētās personas biometriskos datus, kas atrodami dažādās sistēmās, tā vietā, lai izmantotu vairākus komponentus. Kopējam *BMS* būtu jāveicina drošība, kā arī jārada finansiāli, ar uzturēšanu saistīti un operatīvi ieguvumi. Visas automatizētās pirkstu nospiedumu identifikācijas sistēmas, tostarp tās, kas pašlaik tiek izmantotas *Eurodac*, VIS un *SIS*, izmanto biometriskās veidnes, kurās ir dati, kas iegūti faktisko biometrisko paraugu iezīmju izgūšanas rezultātā. Kopējam *BMS* būtu jāpārgrupē un jāglabā visas šīs biometriskās veidnes vienā vietā, tās loģiski nodalot pēc informācijas sistēmas, no kuras dati ir iegūti, tādējādi atvieglojot salīdzināšanu starp dažādām sistēmām ar biometriskajām veidnēm un ļaujot gūt apjomradītus ietaupījumus ES centrālo sistēmu izstrādē un uzturēšanā.

([4]) 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.).

([5]) 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.).

([6]) Padomes Kopējā nostāja 2005/69/TI (2005. gada 24. janvāris) par konkrētu datu apmaiņu ar Interpolu (OV L 27, 29.1.2005, 61. lpp.).

([7]) 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.)

(19) Kopējā *BMS* glabātajām biometriskajām veidnēm būtu jāsastāv no datiem, kas atvasināti faktisko biometrisko paraugu iezīmju izgūšanas rezultātā un iegūti tādā veidā, ka šis izgūšanas process ir neatgriezenisks. Biometriskās veidnes būtu jāiegūst no biometriskajiem datiem, taču nevajadzētu būt iespējamam tos pašus biometriskos datus iegūt no biometriskajām veidnēm. Tā kā plaukstas nospiedumi un DNS profili tiek glabāti tikai *SIS*, izmantoti tikai *SIS* vajadzībām un tos nevar izmantot salīdzināšanai ar datiem citās informācijas sistēmās, ievērojot nepieciešamības un proporcionalitātes principus, kopējā *BMS* nebūtu jāglabā DNS profili vai biometriskās veidnes, kas iegūtas no plaukstas nospiedumu datiem.

(20) Biometriskie dati ir sensitīvi personas dati. Ar šo regulu būtu jānosaka pamats un drošības pasākumi šādu datu apstrādei nolūkā unikāli identificēt attiecīgās personas.

(21) IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN* nepieciešama precīza to personu identifikācija, kuru dati tajās tiek glabāti. Tāpēc *CIR* būtu jāatvieglo minētajās sistēmās reģistrēto personu pareiza identifikācija.

(22) Minētajās ES informācijas sistēmās glabātie personas dati var attiekties uz vienām un tām pašām personām, taču ar atšķirīgām vai nepilnīgām identitātēm. Dalībvalstu rīcībā ir efektīvi līdzekļi, kā savā teritorijā identificēt savus pilsoņus vai reģistrētos pastāvīgos iedzīvotājus. ES informācijas sistēmu sadarbspējai būtu jāpalīdz pareizi identificēt personas, kas tajās atrodamas. *CIR* būtu jāglabā personas dati, kas ir vajadzīgi, lai varētu precīzāk identificēt personas, kuru dati tiek glabāti minētajās sistēmās, tostarp viņu identitātes dati, ceļošanas dokumentu dati un biometriskie dati – neatkarīgi no tā, kurā sistēmā šie dati bija sākotnēji vākti. *CIR* būtu jāglabā tikai tie personas dati, kas ir noteikti vajadzīgi, lai veiktu precīzu identitātes pārbaudi. *CIR* reģistrētie personas dati būtu jāglabā ne ilgāk, kā tas ir noteikti nepieciešams pamatā esošo sistēmu nolūkos, un tie būtu automātiski jādzēš brīdī, kad datus dzēš pamatā esošajās sistēmās saskaņā ar šo datu loģisko nošķirumu.

(23) Ir vajadzīga jauna apstrādes darbība, kas izpaužas kā šādu datu glabāšana *CIR*, nevis katrā atsevišķā sistēmā, lai būtu iespējams paaugstināt identifikācijas precizitāti, izmantojot datu automatizētu salīdzināšanu un atbilstību konstatēšanu. Tam, ka identitātes dati, ceļošanas dokumenta dati un biometriskie dati tiek glabāti *CIR*, nekādi nebūtu jākavē datu apstrāde IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN* nolūkos, jo *CIR* vajadzētu būt minēto pamatā esošo sistēmu jaunam kopīgam komponentam.

(24) Tāpēc nepieciešams *CIR* izveidot individuālu datni par katru personu, kura reģistrēta IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, lai sasniegtu mērķi Šengenas zonas iekšienē pareizi identificēt personas un atbalstīt *MID* nolūkā sasniegt divējādu mērķi, proti, atvieglot *bona fide* ceļotāju identitātes pārbaudes un apkarot identitātes viltošanu. Individuālajai datnei būtu jāglabā vienā vienīgā vietā visa ar personu saistītā identitātes informācija un jādara tā pieejama pienācīgi pilnvarotiem galalietotājiem.

(25) Tādējādi *CIR* būtu jāatvieglo un jāracionalizē par teroristu nodarījumu un citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu vai izmeklēšanu atbildīgo iestāžu piekļuve tādām ES informācijas sistēmām, kuras nav izveidotas tikai un vienīgi tam, lai novērstu, atklātu vai izmeklētu smagus noziegumus.

(26) Ar *CIR* būtu jāizveido kopīga personu, kuras reģistrētas IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN*, identitātes datu, ceļošanas dokumentu datu un biometrisko datu krātuve. Tam vajadzētu ietilpt minēto sistēmu tehniskajā arhitektūrā un darboties kā to kopīgam komponentam identitātes datu, ceļošanas dokumentu datu un biometrisko datu, kurus tās apstrādā, glabāšanai un vaicājumu veikšanai tajās.

(27) Visi *CIR* esošie ieraksti būtu loģiski jānodala, automātiski marķējot katru ierakstu ar tās pamatā esošās sistēmas nosaukumu, kurai minētais ieraksts pieder. Kontrolei attiecībā uz piekļuvi *CIR* būtu jāizmanto šie marķējumi, lai noteiktu, vai atļaut piekļuvi ierakstam.

(28) Ja dalībvalsts policijas iestāde nespēj identificēt personu, jo tai nav ceļošanas dokumenta vai cita ticama dokumenta, kas apliecinātu personas identitāti, vai ja pastāv šaubas par minētās personas sniegtajiem identitātes datiem vai par ceļošanas dokumenta autentiskumu, vai tā turētāja identitāti, vai ja attiecīgā persona nav spējīga

vai atsakās sadarboties, šai policijas iestādei vajadzētu būt iespējai veikt vaicājumu *CIR*, lai identificētu attiecīgo personu. Šajā nolūkā policijas iestādēm pirkstu nospiedumi būtu jāiegūst ar tiešās skenēšanas pirkstu nospiedumu ņemšanas metodēm – ar noteikumu, ka procedūra tika sākta attiecīgās personas klātbūtnē. Šādi vaicājumi *CIR* nebūtu jāatļauj nolūkā identificēt nepilngadīgos, kas ir jaunāki par 12 gadiem, izņemot gadījumus, kad tas ir bērna interesēs.

(29) Ja personas biometriskie dati nav izmantojami vai ja vaicājums uz šo datu pamata nav rezultatīvs, vaicājums būtu jāveic, izmantojot minētās personas identitātes datus apvienojumā ar ceļošanas dokumenta datiem. Gadījumos, kad vaicājuma rezultātā noskaidrojas, ka dati par minēto personu tiek glabāti *CIR*, dalībvalstu iestādēm vajadzētu būt piekļuvei *CIR*, lai aplūkotu minētās personas identitātes datus un ceļošanas dokumenta datus, *CIR* nesniedzot nekādu norādi par to, kurai ES informācijas sistēmai dati pieder.

(30) Dalībvalstīm būtu jāpieņem valsts tiesību akti, ar kuriem nosaka iestādes, kas ir kompetentas veikt identitātes pārbaudes, izmantojot *CIR*, un nosakot šādu pārbaužu procedūras, nosacījumus un kritērijus, kam būtu jāievēro proporcionalitātes princips. Valsts tiesību aktos jo īpaši būtu jāparedz pilnvaras iegūt biometriskos datus tādas personas identitātes pārbaudes laikā, kura fiziski atrodas pie minēto iestāžu darbinieka.

(31) Ar šo regulu būtu arī jāievieš jauna iespēja, saskaņā ar kuru dalībvalsts izraudzītām iestādēm, kas ir atbildīgas par teroristu nodarījumu un smagu noziedzīgu nodarījumu novēršanu, atklāšanu vai izmeklēšanu, un Eiropolam ir racionalizēta piekļuve datiem, kas ietver ne tikai IIS, VIS, *ETIAS* vai *Eurodac* esošos identitātes vai ceļošanas dokumentu datus. Šādi dati var būt vajadzīgi, lai kādā konkrētā lietā novērstu, atklātu vai izmeklētu teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, ja ir pamatots iemesls uzskatīt, ka datu aplūkošana palīdzēs novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, jo īpaši, ja ir aizdomas, ka persona, ko tur aizdomās par teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu, šāda nodarījuma izdarītājs vai tajā cietušais ir persona, kuras dati tiek glabāti IIS, VIS, *ETIAS* vai *Eurodac*.

(32) Piemērojamiem tiesību instrumentiem arī turpmāk būtu jāreglamentē pilnīga piekļuve IIS, VIS, *ETIAS* vai *Eurodac* esošajiem datiem, kuri vajadzīgi teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanai, atklāšanai vai izmeklēšanai un kuri nav tikai attiecīgie *CIR* ietvertie identitātes dati vai ceļošanas dokumentu dati. Izraudzītās iestādes, kas ir atbildīgas par teroristu nodarījumu un citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu vai izmeklēšanu, un Eiropols iepriekš nezina, kurā ES informācijas sistēmā ir to personu dati, attiecībā uz kurām tām jāveic vaicājums. Tas rada aizkavēšanos un neefektivitāti. Tāpēc izraudzītās iestādes pilnvarotajam galalietotājam būtu jāatļauj redzēt, kurā no minētajām ES informācijas sistēmām ir reģistrēti dati, kas iegūti vaicājuma rezultātā. Tādējādi pēc tam, kad būtu automatizēti verificēta atbilstības esamība sistēmā, attiecīgā sistēma tiktu apzīmēta ar karodziņu (tā dēvētā atbilstības karodziņu funkcija).

(33) Šādā kontekstā atbilde no *CIR* nebūtu jāinterpretē vai jāizmanto kā pamatojums vai iemesls, lai izdarītu secinājumus par personu vai veiktu pret to vērstus pasākumus, un tā būtu jāizmanto tikai, lai iesniegtu pieprasījumu piekļūt pamatā esošajām ES informācijas sistēmām, ievērojot nosacījumus un procedūras, kas paredzētas attiecīgajos tiesību instrumentos, kuri reglamentē šādu piekļuvi. Jebkuram šādam piekļuves pieprasījumam būtu jāpiemēro šīs regulas VII nodaļa un attiecīgi Regula (ES) 2016/679, Direktīva (ES) 2016/680 vai Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 ([8]).

(34) Parasti, ja atbilstības karodziņš rāda, ka dati ir reģistrēti IIS, VIS,*ETIAS* vai *Eurodac*, izraudzītajām iestādēm vai Eiropolam būtu jāpieprasa pilnīga piekļuve vismaz vienai no attiecīgajām ES informācijas sistēmām. Ja izņēmuma gadījumā šāda pilnīga piekļuve netiek pieprasīta, jo, piemēram, izraudzītās iestādes vai Eiropols datus jau ir ieguvušas citādi vai valsts tiesību akti datu iegūšanu vairs neatļauj, būtu jāreģistrē piekļuves nepieprasīšanas pamatojums.

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

(35) Reģistra ierakstos par *CIR* veiktajiem vaicājumiem būtu jānorāda vaicājuma nolūks. Ja šāds vaicājums tika veikts, izmantojot divpakāpju pieeju datu aplūkošanai, reģistra ierakstos būtu jāiekļauj atsauce uz izmeklēšanas vai lietas valsts datni, tādējādi norādot, ka šāds vaicājums tiks sākts teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, atklāšanas vai izmeklēšanas nolūkā.

(36) Lai izraudzītā iestāde un Eiropols varētu veikt vaicājumu *CIR* ar nolūku iegūt atbilstības karodziņa veida atbildi, kurā norādīts, ka dati ir reģistrēti IIS, VIS, *ETIAS* vai *Eurodac*, ir nepieciešama automatizēta personas datu apstrāde. Atbilstības karodziņam nebūtu jāatklāj attiecīgās personas personas dati, izņemot to, ka daļa no šīs personas datiem tiek glabāti vienā no sistēmām. Pilnvarotajam galalietotājam nebūtu jāpieņem nekādi nelabvēlīgi lēmumi attiecībā uz attiecīgo personu, pamatojoties vienīgi uz atbilstības karodziņa vienkāršu parādīšanos. Tādēļ piekļuve, kura piešķirta atbilstības karodziņa galalietotājam, radīs ļoti ierobežotu iejaukšanos attiecīgās personas tiesībās uz personas datu aizsardzību, vienlaikus atļaujot izraudzītajām iestādēm un Eiropolam efektīvāk pieprasīt piekļuvi personas datiem.

(37) Būtu jāizveido *MID*, lai sekmētu *CIR* darbību un atbalstītu IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus. Lai visas šīs ES informācijas sistēmas būtu efektīvas savu attiecīgo mērķu izpildē, tām ir nepieciešama precīza to personu identifikācija, kuru personas dati tajās tiek glabāti.

(38) Lai labāk sasniegtu ES informācijas sistēmu mērķus, iestādēm, kas izmanto šīs sistēmas, vajadzētu būt iespējai veikt pietiekami ticamas tādu personu identitātes verifikācijas, kuru dati tiek glabāti dažādās sistēmās. Konkrētajā atsevišķajā sistēmā glabāto identitātes vai ceļošanas dokumentu datu kopums var būt nepareizs, nepilnīgs vai maldinošs, un pašlaik nav iespējas konstatēt nepareizus, nepilnīgus vai maldinošus identitātes vai ceļošanas dokumentu datus, veicot salīdzināšanu ar citā sistēmā glabātiem datiem. Lai šo situāciju labotu, Savienības līmenī ir vajadzīgs tehnisks instruments, kas šajos nolūkos ļautu precīzi identificēt personas.

(39) Ar *MID* būtu jāizveido un jāglabā saiknes starp datiem dažādās ES informācijas sistēmās, lai konstatētu vairākas identitātes, nolūkā sasniegt divējādu mērķi, proti, atvieglot *bona fide* ceļotāju identitātes pārbaudes un apkarot identitātes viltošanu. *MID* būtu jāietver tikai saiknes starp datiem attiecībā uz personām, kuras atrodamas vairāk nekā vienā ES informācijas sistēmā. Saistītie dati būtu stingri jāierobežo, ietverot tikai tos, kas vajadzīgi, lai pārbaudītu, vai attiecīgā persona dažādās sistēmās pamatoti vai nepamatoti ir reģistrēta ar dažādām identitātēm, vai precizētu, ka divas personas ar līdzīgiem identitātes datiem var nebūt viena un tā pati persona. Datu apstrāde, ko veic, izmantojot *ESP* un kopējo *BMS*, lai saistītu individuālas personu datnes atsevišķu sistēmu starpā, būtu jānotur absolūta minimuma robežās, un tāpēc jāizmanto tikai vairāku identitāšu konstatēšanai, kas veicama, kad kāda no sistēmām, kuras dati tiek glabāti *CIR* vai pievienoti *SIS*, tiek papildināta ar jauniem datiem. *MID* būtu jāietver drošības pasākumi pret iespējamu diskrimināciju un nelabvēlīgiem lēmumiem attiecībā uz personām ar vairākām likumīgām identitātēm.

(40) Ar šo regulu tiek noteiktas jaunas datu apstrādes darbības, kuru mērķis ir pareizi identificēt attiecīgās personas. Tā ir iejaukšanās viņu pamattiesībās, kas tiek aizsargātas ar Eiropas Savienības Pamattiesību hartas 7. un 8. pantu. Tā kā efektīva ES informācijas sistēmu īstenošana ir atkarīga no pareizas attiecīgo personu identifikācijas, šāda iejaukšanās ir pamatota ar tiem pašiem mērķiem, kuru dēļ katra no šīm sistēmām ir izveidota, proti, ar efektīvu Savienības robežu pārvaldību, Savienības iekšējo drošību un Savienības patvēruma un vīzu politikas efektīvu īstenošanu.

(41) *ESP* un kopējam *BMS* būtu jāsalīdzina *CIR* un *SIS* esošie dati par personām, kad valsts iestāde vai Savienības aģentūra izveido vai augšupielādē jaunus ierakstus. Šādai salīdzināšanai vajadzētu būt automatizētai. *CIR* un *SIS* būtu jāizmanto kopējais *BMS*, lai atklātu iespējamas saiknes, kuru pamatā ir biometriskie dati. *CIR* un *SIS* būtu jāizmanto *ESP*, lai atklātu iespējamas saiknes, kuru pamatā ir burtciparu dati. *CIR* un *SIS* būtu jāvar identificēt vairākās sistēmās glabātus tādus pašus vai līdzīgus datus par personu. Tādā gadījumā būtu jāizveido saikne, kas norāda, ka tā ir viena un tā pati persona. *CIR* un *SIS* būtu jākonfigurē tā, lai nelielas transliterācijas vai pareizrakstības kļūdas tiktu atklātas tādā veidā, kas attiecīgajai personai neradītu nekādus nepamatotus šķēršļus.

(42) Valsts iestādei vai Savienības aģentūrai, kas reģistrēja datus attiecīgajā ES informācijas sistēmā, būtu jāapstiprina vai jāmaina šīs saiknes. Šai valsts iestādei vai Savienības aģentūrai atšķirīgu identitāšu manuālas verifikācijas nolūkā vajadzētu būt piekļuvei datiem, kas tiek glabāti *CIR* vai *SIS* un *MID*.

(43) Atšķirīgu identitāšu manuāla verifikācija būtu jāveic iestādei, kura izveidoja vai atjaunināja datus, kas izraisīja atbilstības rādījumu, kura rezultātā tika izveidota saikne ar citā ES informācijas sistēmā jau glabātajiem datiem. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai iestādei būtu jānovērtē, vai pastāv vairākas identitātes, kas pamatoti vai nepamatoti attiecas uz vienu un to pašu personu. Šāds novērtējums iespēju robežās būtu jāveic attiecīgās personas klātbūtnē, vajadzības gadījumā pieprasot papildu paskaidrojumus vai informāciju. Novērtējums būtu jāveic nekavējoties un saskaņā ar juridiskajām prasībām par informācijas precizitāti, ko paredz Savienības un valsts tiesību akti. Jo īpaši pie robežām iesaistīto personu kustība verifikācijas gaitā tiks ierobežota, tāpēc tā nedrīkstētu ilgt nenoteiktu laiku. Dzeltenas saiknes esamība *MID* pati par sevi nedrīkstētu būt pamats atteikt ieceļošanu, un visi lēmumi par ieceļošanas atļaušanu vai atteikšanu būtu jāpieņem, vienīgi pamatojoties uz piemērojamiem Eiropas Parlamenta un Padomes Regulas (ES) 2016/399 ([9]) noteikumiem.

(44) Attiecībā uz saiknēm, kuras iegūtas saistībā ar *SIS* brīdinājumiem par personām, ko meklē, lai apcietinātu nolūkā tās nodot vai izdot, par pazudušām personām vai neaizsargātām personām, par personām, ko cenšas atrast, lai tās varētu palīdzēt tiesas procesā, vai par personām diskrētu pārbaužu, izmeklēšanas pārbaužu vai īpašu pārbaužu vajadzībām, par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai iestādei vajadzētu būt tās dalībvalsts *SIRENE* birojam, kura izveidoja brīdinājumu. Minēto kategoriju *SIS* brīdinājumi ir sensitīvi un nebūtu obligāti jāizpauž iestādēm, kas izveido vai atjaunina ar tiem saistītos datus vienā no pārējām ES informācijas sistēmām. Saiknes ar *SIS* datiem izveidei nebūtu jāskar darbības, kas ir jāveic saskaņā ar Eiropas Parlamenta un Padomes Regulām (ES) 2018/1860 ([10]), (ES) 2018/1861 ([11]) un (ES) 2018/1862 ([12]).

(45) Šādu saikņu izveidē ir vajadzīga pārredzamība attiecībā pret to skartajām personām. Lai atvieglotu nepieciešamo drošības pasākumu īstenošanu saskaņā ar piemērojamiem Savienības datu aizsardzības noteikumiem, personas, par kurām pēc atšķirīgu identitāšu manuālas verifikācijas ir izveidota sarkana vai balta saikne, būtu rakstiski jāinformē, neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību vai sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta valsts veikta izmeklēšana. Minētajām personām būtu jāsaņem vienots identifikācijas numurs, kas dotu iespēju identificēt iestādi, kurā tām jāvēršas, lai izmantotu savas tiesības.

(46) Ja ir izveidota dzeltena saikne, iestādei, kas atbildīga par atšķirīgu identitāšu manuālu verifikāciju, vajadzētu būt piekļuvei *MID*. Ja pastāv sarkana saikne, dalībvalstu iestādēm un Savienības aģentūrām, kurām ir piekļuve vismaz vienai *CIR* iekļautajai ES informācijas sistēmai vai *SIS*, vajadzētu būt piekļuvei *MID*. Sarkanajai saiknei būtu jānorāda, ka persona nepamatoti izmanto atšķirīgas identitātes vai ka persona izmanto svešu identitāti.

(47) Ja pastāv balta vai zaļa saikne starp datiem divās ES informācijas sistēmās, dalībvalstu iestādēm un Savienības aģentūrām vajadzētu būt piekļuvei *MID*, ja attiecīgajai iestādei vai aģentūrai ir piekļuve abām informācijas sistēmām. Šāda piekļuve būtu jāpiešķir tikai un vienīgi nolūkā ļaut minētajai iestādei vai aģentūrai atklāt potenciālus gadījumus, kad dati ir saistīti nepareizi vai tie apstrādāti *MID*, *CIR* un *SIS*, pārkāpjot šo regulu, un veikt darbības, lai labotu situāciju un atjauninātu vai dzēstu saikni.

([9]) 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.).

([10]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1860 (2018. gada 28. novembris) par Šengenas informācijas sistēmas izmantošanu to trešo valstu valstspiederīgo atgriešanai, kuri dalībvalstīs uzturas nelikumīgi (OV L 312, 7.12.2018., 1. lpp.).

([11]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1861 (2018. gada 28. novembris) 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 312, 7.12.2018., 14. lpp.).

([12]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1862 (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 (OV L 312, 7.12.2018., 56. lpp.).

(48) Eiropas Savienības Aģentūrai lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) būtu jāievieš automatizēti datu kvalitātes kontroles mehānismi un kopēji datu kvalitātes indikatori. *eu-LISA* vajadzētu būt pienākumam attīstīt centrālu spēju datu kvalitātes pārraudzībai un sagatavot regulārus datu analīzes ziņojumus nolūkā uzlabot kontroli pār to, kā dalībvalstis īsteno ES informācijas sistēmas. Kopējiem datu kvalitātes indikatoriem būtu jāietver minimālie kvalitātes standarti attiecībā uz datu glabāšanu ES informācijas sistēmās vai sadarbspējas komponentos. Šādu datu kvalitātes standartu mērķim vajadzētu būt panākt, ka ES informācijas sistēmas un sadarbspējas komponenti var automātiski identificēt acīmredzami kļūdainus vai nekonsekventus ievadītos datus, kā rezultātā izcelsmes dalībvalsts varētu verificēt šos datus un veikt visas vajadzīgās korektīvās darbības.

(49) Komisijai būtu jāizvērtē *eu-LISA* kvalitātes ziņojumi un vajadzības gadījumā jāsniedz ieteikumi dalībvalstīm. Dalībvalstīm vajadzētu būt pienākumam sagatavot rīcības plānu, kurā aprakstītas darbības visu ar datu kvalitāti saistīto trūkumu novēršanai, un būtu regulāri jāziņo par progresu šā rīcības plāna īstenošanā.

(50) Vienotajam ziņojuma formātam (*UMF*) būtu jākalpo kā standartam strukturētai pārrobežu informācijas apmaiņai starp informācijas sistēmām, iestādēm vai organizācijām tieslietu un iekšlietu jomā. *UMF* būtu jānosaka kopēja terminoloģija un loģiskās struktūras attiecībā uz kopīgi apmainītu informāciju, lai atvieglotu sadarbspēju, ļaujot saskaņotā un semantiski līdzvērtīgā veidā izveidot un lasīt apmainītās informācijas saturu.

(51) Var apsvērt iespēju *UMF* standartu izmantot VIS, *SIS* un jebkuros citos esošos vai jaunos pārrobežu informācijas apmaiņas modeļos un informācijas sistēmās, ko dalībvalstis izstrādājušas tieslietu un iekšlietu jomā.

(52) Būtu jāizveido centrāls ziņošanas un statistikas repozitorijs (*CRRS*), lai politikas, operatīvos un datu kvalitātes nolūkos saskaņā ar piemērojamiem tiesību instrumentiem iegūtu vairākas sistēmas aptverošus statistikas datus un analītiskus ziņojumus. *eu-LISA* būtu jāizveido, jāīsteno un jāmitina *CRRS* savos tehniskajos centros. Tajā būtu jāietver anonimizēti statistikas dati no ES informācijas sistēmām, *CIR*, *MID* un kopējā *BMS*. *CRRS* ietvertajiem datiem nebūtu jādod iespēja identificēt atsevišķas personas. *eu-LISA* būtu automatizēti jāpadara dati anonīmi un jāreģistrē šādi anonimizēti dati *CRRS*. Datu anonimizācijas procesam vajadzētu būt automatizētam, un *eu-LISA* darbiniekiem nebūtu jāpiešķir tieša piekļuve ES informācijas sistēmās vai sadarbspējas komponentos glabātiem personas datiem.

(53) Personas datu apstrādei sadarbspējas nolūkā, ko valstu iestādes veic saskaņā ar šo regulu, piemēro Regulu (ES) 2016/679, ja vien šādu apstrādi dalībvalstu izraudzītās iestādes vai centrālie piekļuves punkti neveic teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, atklāšanas vai izmeklēšanas nolūkos.

(54) Ja dalībvalstu veiktu personas datu apstrādi atbilstīgi šai regulai sadarbspējas nolūkā veic kompetentās iestādes teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, atklāšanas vai izmeklēšanas nolūkos, piemēro Direktīvu (ES) 2016/680.

(55) Jebkādu personas datu nosūtīšanai uz trešām valstīm vai starptautiskajām organizācijām, ko veic atbilstīgi šai regulai, piemēro arī Regulu (ES) 2016/679, Regulu (ES) 2018/1725 vai attiecīgos gadījumos Direktīvu (ES) 2016/680. Neskarot Regulas (ES) 2016/679 V nodaļā vai attiecīgā gadījumā Direktīvā (ES) 2016/680 paredzētos nosūtīšanas pamatus, ikviens trešās valsts tiesas spriedums un ikviens trešās valsts administratīvās iestādes lēmums, kurā pārzinim vai apstrādātājam pieprasīts nosūtīt vai izpaust personas datus, būtu jāatzīst vai jāizpilda vienīgi tad, ja tas ir balstīts uz starptautisku nolīgumu, kas ir spēkā starp pieprasītāju trešo valsti un Savienību vai kādu tās dalībvalsti.

(56) Īpašos datu aizsardzības noteikumus, kas paredzēti Eiropas Parlamenta un Padomes Regulās (ES) 2017/2226 ([13]), (EK) Nr. 767/2008 ([14]) un (ES) 2018/1240 ([15]) un Regulā (ES) 2018/1861, piemēro personas datu apstrādei ar minētajām regulām reglamentētajās sistēmās.

(57) Personas datu apstrādei, ko *eu-LISA* un citas Savienības iestādes un struktūras veic, pildot savus pienākumus saskaņā ar šo regulu, piemēro Regulu (ES) 2018/1725, neskarot Eiropas Parlamenta un Padomes Regulu (ES) 2016/794 ([16]), kuru piemēro personas datu apstrādei, ko veic Eiropols.

(58) Dalībvalstu veiktās personas datu apstrādes likumība būtu jāuzrauga uzraudzības iestādēm, kas minētas Regulā (ES) 2016/679 vai Direktīvā (ES) 2016/680. Eiropas Datu aizsardzības uzraudzītājam būtu jāuzrauga Savienības iestāžu un struktūru darbības, kas saistītas ar personas datu apstrādi. Eiropas Datu aizsardzības uzraudzītājam un uzraudzības iestādēm, uzraugot personas datu apstrādi, ko veic ar sadarbspējas komponentu palīdzību, būtu savstarpēji jāsadarbojas. Lai Eiropas Datu aizsardzības uzraudzītājs varētu pildīt tam ar šo regulu uzticētos uzdevumus, ir vajadzīgi pietiekami papildu resursi, tostarp gan cilvēkresursi, gan finansiālie resursi.

(59) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001 ([17]) 28. panta 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2018. gada 16. aprīlī ([18]) ir sniedzis atzinumu.

(60) 29. panta datu aizsardzības darba grupa sniedza atzinumu 2018. gada 11. aprīlī.

(61) Gan dalībvalstīm, gan *eu-LISA* būtu jāuztur drošības plāns, lai atvieglotu drošības saistību izpildi, un tām būtu jāsadarbojas, lai risinātu drošības jautājumus. *eu-LISA* būtu arī jāgādā par to, ka pastāvīgi tiek izmantoti jaunākie tehnoloģiskie sasniegumi, lai nodrošinātu datu integritāti saistībā ar sadarbspējas komponentu izstrādi, projektēšanu un pārvaldību. Šajā ziņā *eu-LISA* pienākumos vajadzētu būt arī pieņemt pasākumus, kas vajadzīgi, lai liegtu nepilnvarotu personu, piemēram, ārpakalpojumu sniedzēju darbinieku, piekļuvi personas datiem, kuri tiek apstrādāti ar sadarbspējas komponentiem. Piešķirot tiesības slēgt pakalpojumu līgumus, dalībvalstīm un *eu-LISA* būtu jāapsver visi pasākumi, kas vajadzīgi, lai nodrošinātu atbilstību tiesību aktiem vai noteikumiem, kuri saistīti ar personas datu un privātuma aizsardzību, vai sargātu būtiskas drošības intereses, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2018/1046 ([19]) un piemērojamās starptautiskās konvencijas. *eu-LISA* sadarbspējas komponentu izstrādes gaitā būtu jāievēro integrētas privātuma aizsardzības un privātuma aizsardzības pēc noklusējuma principi.

(62) Šajā regulā paredzēto sadarbspējas komponentu īstenošana ietekmēs to, kā robežšķērsošanas vietās tiek veiktas pārbaudes. Šī ietekme izrietēs no pastāvošo Regulas (ES) 2016/399 noteikumu un šajā regulā paredzēto sadarbspējas noteikumu kombinētas piemērošanas.

(63) Šīs kombinētās noteikumu piemērošanas rezultātā Eiropas meklēšanas portālam (*ESP*) vajadzētu būt galvenajam piekļuves punktam, kur robežšķērsošanas vietās par personām veiktu Regulā (ES) 2016/399 paredzēto obligāto sistemātisko meklēšanu datubāzēs. Turklāt, lai novērtētu, vai persona atbilst Regulā (ES) 2016/399 noteiktajiem ieceļošanas nosacījumiem, robežsargiem būtu jāņem vērā identitātes dati vai ceļošanas dokumentu dati, uz kuru

([13]) Eiropas Parlamenta un Padomes Regula (ES) 2017/2226 (2017. gada 30. novembris), ar ko izveido ieceļošanas/izceļošanas sistēmu (IIS), lai reģistrētu to trešo valstu valstspiederīgo ieceļošanas un izceļošanas datus un ieceļošanas atteikumu datus, kuri šķērso Eiropas Savienības dalībvalstu ārējās robežas, un ar ko paredz nosacījumus piekļuvei IIS tiesībaizsardzības nolūkos un groza Konvenciju, ar ko īsteno Šengenas nolīgumu un Regulu (EK) Nr. 767/2008 un Regulu (ES) Nr. 1077/2011 (IIS regula) (OV L 327, 9.12.2017., 20. lpp.).

([14]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 767/2008 (2008. gada 9. jūlijs) par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (VIS regula) (OV L 218, 13.8.2008., 60. lpp.).

([15]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1240 (2018. gada 12. septembris), ar ko izveido Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*) un groza Regulas (ES) Nr. 1077/2011, (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/1624 un (ES) 2017/2226 (OV L 236, 19.9.2018., 1. lpp.).

([16]) 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.).

([17]) 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.).

([18]) OV C 233, 4.7.2018., 12. lpp.

([19]) Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2018/1046 (2018. gada 18. jūlijs) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam, ar kuru groza Regulas (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 un Lēmumu Nr. 541/2014/ES un atceļ Regulu (ES, Euratom) Nr. 966/2012 (OV L 193, 30.7.2018., 1. lpp.).

pamata kāda saikne *MID* ir klasificēta kā sarkana saikne. Tomēr sarkanas saiknes esamība pati par sevi nebūtu uzskatāma par ieceļošanas atteikuma iemeslu, un tāpēc nebūtu jāgroza esošie Regulā (ES) 2016/399 uzskaitītie ieceļošanas atteikuma iemesli.

(64) Būtu lietderīgi atjaunināt Robežsargu rokasgrāmatu, lai padarītu šos precizējumus nepārprotamus.

(65) Ja vaicājuma, kas, izmantojot *ESP*, veikts *MID*, rezultāts ir dzeltena saikne vai tiek atklāta sarkana saikne, tad robežsargam būtu jāaplūko dati *CIR* vai *SIS*, vai abos, lai novērtētu informāciju par pārbaudāmo personu nolūkā manuāli verificēt viņas identitāti un pielāgot saiknes krāsu, ja tas ir nepieciešams.

(66) Lai sekmētu statistikas un ziņošanas mērķus, ir jāpiešķir piekļuve šajā regulā minēto kompetento iestāžu, Savienības iestāžu un aģentūru pilnvarotiem darbiniekiem, lai viņi varētu aplūkot konkrētus ar konkrētiem sadarbspējas komponentiem saistītus datus, nedodot viņiem iespēju identificēt personas.

(67) Lai ļautu dalībvalstu iestādēm un Savienības aģentūrām pielāgoties jaunajām prasībām par *ESP* izmantošanu, ir jāparedz pārejas periods. Līdzīgi, lai nodrošinātu *MID* saskaņotu un optimālu darbību, būtu jānosaka pārejas pasākumi attiecībā uz tā darbības sākumu.

(68) Ņemot vērā to, ka šīs regulas mērķi, proti, izveidot ES informācijas sistēmu sadarbspējas satvaru, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet šīs rīcības mēroga un iedarbības dēļ to 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 minētā mērķa sasniegšanai.

(69) Atlikusī summa budžetā, kurš ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 515/2014 ([20]) ir piešķirts viedrobežām, būtu jāpārdala šai regulai saskaņā ar Regulas (ES) Nr. 515/2014 5. panta 5. punkta b) apakšpunktu, lai segtu sadarbspējas komponentu izstrādes izmaksas.

(70) Lai papildinātu konkrētus detalizētus šīs regulas tehniskos aspektus, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 290. pantu attiecībā uz:

— pārejas perioda pagarināšanu *ESP* izmantošanai,

— pārejas perioda pagarināšanu *ETIAS* centrālās vienības veiktai vairāku identitāšu konstatēšanai,

— procedūrām tādu gadījumu noteikšanai, kad identitāti var uzskatīt par tādu pašu vai līdzīgu,

— noteikumiem par *CRRS* darbību, tostarp īpašiem personas datu apstrādes aizsardzības pasākumiem un drošības noteikumiem, ko piemēro repozitorijam, un

— detalizētiem noteikumiem par tīmekļa portāla darbību.

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 ([21]). 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) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai, lai tā noteiktu datumu, kad *ESP*, kopējam *BMS*, *CIR*, *MID* un *CRRS* jāsāk darbība.

([20]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 515/2014 (2014. gada 16. aprīlis), ar ko kā daļu no Iekšējās drošības fonda izveido finansiāla atbalsta instrumentu ārējām robežām un vīzām un atceļ Lēmumu Nr. 574/2007/EK (OV L 150, 20.5.2014., 143. lpp.).

([21]) OV L 123, 12.5.2016., 1. lpp.

(72) Būtu arī jāpiešķir Komisijai īstenošanas pilnvaras attiecībā uz sīki izstrādātu noteikumu pieņemšanu par: *ESP* lietotāju profilu tehniskajiem parametriem; specifikācijām tehniskajam risinājumam, kas ļauj, izmantojot *ESP*, veikt vaicājumus ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs, un *ESP* atbilžu formātu; tehniskajiem noteikumiem, kā *MID* izveidot saiknes starp datiem no dažādām ES informācijas sistēmām; tādas veidlapas saturu un izklāstu, ko izmanto, lai informētu datu subjektu sarkanas saiknes izveidošanas gadījumā; kopējā *BMS* snieguma prasībām un snieguma uzraudzību; automatizētiem datu kvalitātes kontroles mehānismiem, procedūrām un rādītājiem; *UMF* standarta izstrādi; sadarbības procedūru drošības incidenta gadījumā; tehniskā risinājuma specifikācijām, kurš paredzēts dalībvalstīm lietotāju piekļuves pieprasījumu pārvaldībai. Minētās pilnvaras būtu jāīsteno saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 ([22]).

(73) Tā kā sadarbspējas komponenti ietvers ievērojama sensitīvu personas datu daudzuma apstrādi, ir svarīgi, lai personas, kuru dati tiek apstrādāti, izmantojot minētos komponentus, var efektīvi īstenot savas datu subjektu tiesības, kas noteiktas Regulā (ES) 2016/679, Direktīvā (ES) 2016/680 un Regulā (ES) 2018/1725. Datu subjektu vajadzībām būtu jānodrošina tīmekļa portāls, kas atvieglo viņiem īstenot savas tiesības piekļūt saviem personas datiem un tiesības uz personas datu labošanu, dzēšanu un apstrādes ierobežošanu. Šāds tīmekļa portāls būtu jāizveido un jāpārvalda *eu-LISA*.

(74) Viens no datu aizsardzības pamatprincipiem ir datu minimizēšana: atbilstīgi Regulas (ES) 2016/679 5. panta 1. punkta c) apakšpunktam personas datu apstrādei ir jābūt adekvātai, atbilstīgai un jāietver tikai tas, kas nepieciešams to apstrādes nolūkos. Tāpēc sadarbspējas komponentiem nebūtu jāparedz nekādu jaunu personas datu glabāšana, izņemot saiknes, kas tiks glabātas *MID* un kas ir šīs regulas nolūkiem vajadzīgais minimums.

(75) Šajā regulā būtu jāietver skaidri noteikumi par atbildību un tiesībām uz kompensāciju personas datu nelikumīgas apstrādes un jebkādas citas ar šo regulu nesaderīgas darbības gadījumā. Šādiem noteikumiem nebūtu jāskar tiesības uz kompensāciju no pārziņa vai apstrādātāja un pārziņa vai apstrādātāja atbildību saskaņā ar Regulu (ES) 2016/679, Direktīvu (ES) 2016/680 un Regulu (ES) 2018/1725. *eu-LISA*, kad tā darbojas kā datu apstrādātājs, vajadzētu būt atbildīgai par jebkādu kaitējumu, ko tā izraisījusi gadījumā, ja tā nav izpildījusi konkrētos šīs regulas pienākumus, kas tai izvirzīti, vai rīkojusies ārpus vai pretēji tās dalībvalsts likumīgiem norādījumiem, kura ir datu pārzinis.

(76) Šī regula neskar Eiropas Parlamenta un Padomes Direktīvas 2004/38/EK ([23]) piemērošanu.

(77) 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 papildina 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.

(78) Šī regula ir to Šengenas acquis noteikumu pilnveidošana, kuru īstenošanā Apvienotā Karaliste nepiedalās saskaņā ar Padomes Lēmumu 2000/365/EK ([24]); tādēļ Apvienotā Karaliste nepiedalās šīs regulas pieņemšanā, un Apvienotajai Karalistei šī regula nav saistoša un nav jāpiemēro.

(79) Šī regula ir to Šengenas acquis noteikumu pilnveidošana, kuru īstenošanā Īrija nepiedalās saskaņā ar Padomes Lēmumu 2002/192/EK ([25]); tādēļ Īrija nepiedalās šīs regulas pieņemšanā, un Īrijai šī regula nav saistoša un nav jāpiemēro.

([22]) 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.).

([23]) Eiropas Parlamenta un Padomes Direktīva 2004/38/EK (2004. gada 29. aprīlis) par Savienības pilsoņu un viņu ģimenes locekļu tiesībām brīvi pārvietoties un dzīvot dalībvalstu teritorijā, ar ko groza Regulu (EEK) Nr. 1612/68 un atceļ Direktīvas 64/221/EEK, 68/360/EEK, 72/194/EEK, 73/148/EEK, 75/34/EEK, 75/35/EEK, 90/364/EEK, 90/365/EEK un 93/96/EEK (OV L 158, 30.4.2004., 77. lpp.).

([24]) 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.).

([25]) 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.).

(80) 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 ([26]), šī regula ir to Šengenas acquis noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta 1. panta A, B un G punktā Padomes Lēmumā 1999/437/EK ([27]).

(81) Attiecībā uz Šveici – saskaņā ar Nolīgumu, kas noslēgts starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas acquis īstenošanā, piemērošanā un pilnveidošanā ([28]), šī regula ir to Šengenas acquis noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta Lēmuma 1999/437/EK 1. panta A, B un G punktā, kurus lasa saistībā ar Padomes Lēmuma 2008/146/EK 3. pantu ([29]).

(82) Attiecībā uz Lihtenšteinu – saskaņā ar 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 ([30]), šī regula ir to Šengenas acquis noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta Lēmuma 1999/437/EK 1. panta A, B un G punktā, kurus lasa saistībā ar Padomes Lēmuma 2011/350/ES 3. pantu ([31]).

(83) Šī regula atbilst jo īpaši Eiropas Savienības Pamattiesību hartā atzītajām pamattiesībām un principiem un būtu jāpiemēro saskaņā ar minētajām tiesībām un principiem.

(84) Lai šo regulu ietvertu spēkā esošajā tiesiskajā regulējumā, būtu attiecīgi jāgroza Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumi 2004/512/EK ([32]) un 2008/633/TI ([33]),

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

Vispārīgi noteikumi

1. pants

Priekšmets

1. Ar šo regulu – kopā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/818 ([34]) – izveido satvaru sadarbspējas nodrošināšanai starp ieceļošanas/izceļošanas sistēmu (IIS), vīzu informācijas sistēmu (VIS), Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*), *Eurodac*, Šengenas Informācijas sistēmu (*SIS*) un Eiropas Sodāmības reģistru informācijas sistēmu trešo valstu valstspiederīgajiem (*ECRIS-TCN*).

([26]) OV L 176, 10.7.1999., 36. lpp.
([27]) 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.)
([28]) OV L 53, 27.2.2008., 52. lpp.
([29]) Padomes Lēmums 2008/146/EK (2008. gada 28. janvāris) par to, lai Eiropas Kopienas 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., 1. lpp.).
([30]) OV L 160, 18.6.2011., 21. lpp.
([31]) Padomes Lēmums 2011/350/ES (2011. gada 7. marts) par to, lai Eiropas Savienības vārdā noslēgtu Protokolu starp Eiropas Savienību, Eiropas Kopienu, Šveices Konfederāciju un Lihtenšteinas Firstisti par Lihtenšteinas Firstistes pievienošanos Nolīgumam starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas acquis īstenošanā, piemērošanā un pilnveidošanā saistībā ar kontroles atcelšanu pie iekšējām robežām un personu pārvietošanos (OV L 160, 18.6.2011., 19. lpp.).
([32]) Padomes Lēmums 2004/512/EK (2004. gada 8. jūnijs), ar ko izveido Vīzu informācijas sistēmu (VIS) (OV L 213, 15.6.2004., 5. lpp.).
([33]) Padomes Lēmums 2008/633/TI (2008. gada 23. jūnijs) par izraudzīto dalībvalstu iestāžu un Eiropola piekļuvi Vīzu informācijas sistēmai (VIS) konsultāciju nolūkos, lai novērstu, atklātu un izmeklētu teroristu nodarījumus un citus smagus noziedzīgus nodarījumus (OV L 218, 13.8.2008., 129. lpp.).
([34]) Eiropas Parlamenta un Padomes Regula (ES) 2019/818 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai policijas un tiesu iestāžu sadarbības, patvēruma un migrācijas jomā un groza Regulas (ES) 2018/1726, (ES) 2018/1862 un (ES) 2019/816 (skatīt šā *Oficiālā Vēstneša* 85. lpp.).

2. Satvars ietver šādus sadarbspējas komponentus:

a) Eiropas meklēšanas portāls (*ESP*);

b) kopējs biometrisko datu salīdzināšanas pakalpojums (kopējais *BMS*);

c) kopējs identitātes repozitorijs (*CIR*);

d) vairāku identitāšu detektors (*MID*).

3. Šajā regulā ir arī paredzēti noteikumi par datu kvalitātes prasībām, vienotu ziņojuma formātu (*UMF*) un centrālu ziņošanas un statistikas repozitoriju (*CRRS*) un ir noteikti dalībvalstu un Eiropas Aģentūras lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) pienākumi attiecībā uz sadarbspējas komponentu uzbūvi, izstrādi un darbību.

4. Ar šo regulu arī pielāgo procedūras un nosacījumus, ko piemēro dalībvalstu izraudzīto iestāžu un Eiropas Savienības Aģentūras tiesībaizsardzības sadarbībai (Eiropola) piekļuvei IIS, VIS, *ETIAS* un *Eurodac* ar mērķi novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus.

5. Šī regula paredz arī satvaru personu identitātes verificēšanai un personu identificēšanai.

2. pants

Mērķi

1. Nodrošinot sadarbspēju, šai regulai ir šādi mērķi:

a) uzlabot robežpārbaužu iedarbīgumu un efektivitāti uz ārējām robežām;

b) sekmēt nelikumīgas imigrācijas novēršanu un apkarošanu;

c) sekmēt augsta drošības līmeņa panākšanu Savienības brīvības, drošības un tiesiskuma telpā, tostarp sabiedriskās drošības un sabiedriskās kārtības uzturēšanu un drošības saglabāšanu dalībvalstu teritorijās;

d) uzlabot kopējās vīzu politikas īstenošanu;

e) palīdzēt starptautiskās aizsardzības pieteikumu izskatīšanā;

f) palīdzēt novērst, atklāt un izmeklēt teroristu nodarījumus un citus smagus noziedzīgus nodarījumus;

g) palīdzēt identificēt nezināmas personas, kuras sevi identificēt nespēj, vai neidentificētas cilvēku mirstīgās atliekas dabas katastrofas, nelaimes gadījuma vai teroristu uzbrukuma gadījumā.

2. Šā panta 1. punkta minētos mērķus sasniedz:

a) nodrošinot personu pareizu identifikāciju;

b) palīdzot apkarot identitātes viltošanu;

c) uzlabojot datu kvalitāti un saskaņojot prasības par ES informācijas sistēmās glabāto datu kvalitāti, vienlaikus ievērojot datu apstrādes prasības, kas noteiktas tiesību instrumentos, kuri reglamentē atsevišķās sistēmas, kā arī datu aizsardzības standartus un principus;

d) atvieglojot un atbalstot esošo ES informācijas sistēmu tehnisko un operatīvo īstenošanu dalībvalstīs;

e) pastiprinot, vienkāršojot un padarot saskaņotākus datu drošības un datu aizsardzības nosacījumus, kuri reglamentē attiecīgās ES informācijas sistēmas, taču neietekmējot īpašo aizsardzību un aizsardzības pasākumus, kas ir paredzēti konkrētām datu kategorijām;

f) racionalizējot nosacījumus par izraudzīto iestāžu piekļuvi IIS, VIS, *ETIAS* un *Eurodac* sistēmām, vienlaikus nodrošinot nepieciešamus un samērīgus minētās piekļuves nosacījumus;

g) atbalstot IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

3. pants

Darbības joma

1. Šo regulu piemēro IIS, VIS, *ETIAS* un *SIS*.

2. Šo regulu piemēro personām, attiecībā uz kurām personas datus var apstrādāt šā panta 1. punktā minētajās ES informācijas sistēmās un kuru dati tiek vākti nolūkos, kas noteikti Regulas (EK) Nr. 767/2008 1. un 2. pantā, Regulas (ES) 2017/2226 1. pantā, Regulas (ES) 2018/2140 1. un 4. pantā, Regulas (ES) 2018/1860 1. pantā un Regulas (ES) 2018/1861 1. pantā.

4. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "ārējās robežas" ir ārējās robežas, kā definēts Regulas (ES) 2016/399 2. panta 2) punktā;

2) "robežpārbaudes" ir robežpārbaudes, kā definēts Regulas (ES) 2016/399 2. panta 11) punktā;

3) "robežu iestāde" ir robežsardze, kurai saskaņā ar valsts tiesību aktiem ir uzdots veikt robežpārbaudes;

4) "uzraudzības iestādes" ir uzraudzības iestāde, kas minēta Regulas (ES) 2016/679 51. panta 1. punktā, un uzraudzības iestāde, kas minēta Direktīvas (ES) 2016/680 41. panta 1. punktā;

5) "verifikācija" ir datu kopumu salīdzināšana nolūkā apstiprināt uzdotu identitāti (pārbaude "viens pret vienu");

6) "identifikācija" ir personas identitātes noteikšana, meklējot datubāzē un salīdzinot ar daudziem datu kopumiem (pārbaude "viens pret daudziem");

7) "burtciparu dati" ir dati, ko veido burti, cipari, īpašas zīmes, atstarpes un pieturzīmes;

8) "identitātes dati" ir dati, kas minēti 27. panta 3. punkta a)–e) apakšpunktā;

9) "pirkstu nospiedumu dati" ir pirkstu nospiedumu attēli un latentu pirkstu nospiedumu attēli, kuri, ņemot vērā to unikālās īpašības un tajos ietvertās atsauces vērtības, dara iespējamu precīzu un pārliecinošu salīdzināšanu attiecībā uz personas identitāti;

10) "sejas attēls" ir digitāls personas sejas attēls;

11) "biometriskie dati" ir pirkstu nospiedumu dati vai sejas attēli, vai abi;

12) "biometriskā veidne" ir matemātisks attēlojums, kas iegūts no biometriskajiem datiem iezīmju izguves rezultātā un aprobežojas ar pazīmēm, kuras ir vajadzīgas identifikācijas un verifikācijas veikšanai;

13) "ceļošanas dokuments" ir pase vai cits līdzvērtīgs dokuments, kas tā turētājam dod tiesības šķērsot ārējās robežas un kam var piestiprināt vīzu;

14) "ceļošanas dokumenta dati" ir ceļošanas dokumenta veids, numurs un tā izdevēja valsts, ceļošanas dokumenta derīguma beigu termiņš un ceļošanas dokumenta izdevējas valsts trīs burtu kods;

15) "ES informācijas sistēmas" ir IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN*;

16) "Eiropola dati" ir personas dati, ko Eiropols apstrādājis Regulas (ES) 2016/794 18. panta 2. punkta a), b) un c) apakšpunktā minētajos nolūkos;

17) "Interpola datubāzes" ir Interpola Zagto un pazaudēto ceļošanas dokumentu (*SLTD* datubāze) datubāze un Interpola datubāze ar ceļošanas dokumentiem, par kuriem izdoti paziņojumi (*TDAWN* datubāze);

18) "atbilstība" ir atbilsme, kas ir konstatēta, automātiski salīdzinot personas datus, kuri ir reģistrēti vai tiek reģistrēti kādā informācijas sistēmā vai datubāzē;

19) "policijas iestāde" ir "kompetentā iestāde", kā definēts Direktīvas (ES) 2016/680 3. panta 7) punktā;

20) "izraudzītās iestādes" ir dalībvalstu izraudzītās iestādes, kas definētas Regulas (ES) 2017/2226 3. panta 1. punkta 26) apakšpunktā, Lēmuma 2008/633/TI 2. panta 1. punkta e) apakšpunktā un Regulas (ES) 2018/1240 3. panta 1. punkta 21) apakšpunktā;

21) "teroristu nodarījums" ir valsts tiesību aktos minēts nodarījums, kas atbilst vai ir līdzvērtīgs vienam no nodarījumiem, kuri minēti Eiropas Parlamenta un Padomes Direktīvā (ES) 2017/541 ([35]);

22) "smags noziedzīgs nodarījums" ir nodarījums, kas atbilst vai ir līdzvērtīgs vienam no nodarījumiem, kuri minēti Padomes Pamatlēmuma 2002/584/TI ([36]) 2. panta 2. punktā, ja tas saskaņā ar valsts tiesību aktiem ir sodāms ar brīvības atņemšanu vai ar brīvības atņemšanu saistītu drošības līdzekli, kura maksimālais ilgums ir vismaz trīs gadi;

23) "ieceļošanas/izceļošanas sistēma" jeb "IIS" ir ieceļošanas/izceļošanas sistēma, kas izveidota ar Regulu (ES) 2017/2226;

24) "vīzu informācijas sistēma" jeb "VIS" ir vīzu informācijas sistēma, kas izveidota ar Regulu (EK) Nr. 767/2008;

25) "Eiropas ceļošanas informācijas un atļauju sistēma" jeb "*ETIAS*" ir Eiropas ceļošanas informācijas un atļauju sistēma, kas izveidota ar Regulu (ES) 2018/1240;

26) "*Eurodac*" ir *Eurodac*, kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 603/2013 ([37]);

27) "Šengenas informācijas sistēma" jeb "*SIS*" ir Šengenas Informācijas sistēma, kas izveidota ar Regulām (ES) 2018/1860, (ES) 2018/1861 un (ES) 2018/1862;

28) "*ECRIS-TCN*" ir centralizētā sistēma, ar ko apzina dalībvalstis, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/816 ([38]).

5. pants

Nediskriminēšana un pamattiesības

Personas datu apstrāde, ko veic šīs regulas vajadzībām, neizraisa nekādu diskrimināciju pret personām, arī ne tādu iemeslu dēļ kā dzimums, rase, ādas krāsa, etniskā vai sociālā izcelsme, ģenētiskās īpatnības, valoda, reliģija vai pārliecība, politiski vai citi uzskati, piederība pie nacionālas minoritātes, īpašums, izcelsme, invaliditāte, vecums vai seksuālā orientācija. Tā pilnībā respektē cilvēka cieņu un integritāti, kā arī pamattiesības, tostarp tiesības uz privāto dzīvi un personas datu aizsardzību. Īpašu uzmanību pievērš bērniem, veciem cilvēkiem, personām ar invaliditāti un personām, kurām ir nepieciešama starptautiskā aizsardzība. Primāri ņem vērā bērna intereses.

II NODAĻA

Eiropas meklēšanas portāls

6. pants

Eiropas meklēšanas portāls

1. Tiek izveidots Eiropas meklēšanas portāls (*ESP*), lai atvieglotu dalībvalstu iestāžu un Savienības aģentūru ātru, netraucētu, efektīvu, sistemātisku un kontrolētu piekļuvi ES informācijas sistēmām, Eiropola datiem un Interpola datubāzēm to uzdevumu veikšanai un saskaņā ar to piekļuves tiesībām un IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķiem un nolūkiem.

([35]) 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.).

([36]) 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.).

([37]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 603/2013 (2013. gada 26. jūnijs) par pirkstu nospiedumu salīdzināšanas sistēmas *Eurodac* izveidi, lai efektīvi piemērotu Regulu (ES) Nr. 604/2013, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm, un par dalībvalstu tiesībaizsardzības iestāžu un Eiropola pieprasījumiem veikt salīdzināšanu ar *Eurodac* datiem tiesībaizsardzības nolūkos, un ar kuru groza Regulu (ES) Nr. 1077/2011, ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (OV L 180, 29.6.2013., 1. lpp.).

([38]) Eiropas Parlamenta un Padomes Regula (ES) 2019/816 (2019. gada 17. aprīlis), ar ko Eiropas Sodāmības reģistru informācijas sistēmas papildināšanai un atbalstam izveido centralizētu sistēmu (*ECRIS-TCN* sistēma) tādu dalībvalstu identificēšanai, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un ar ko groza Regulu (ES) 2018/1726 (skatīt šā *Oficiālā Vēstneša* 1. lpp.).

2. *ESP* veido:

a) centrāla infrastruktūra, tostarp meklēšanas portāls, kas ļauj vienlaikus veikt vaicājumus IIS, VIS, *ETIAS*, *Eurodac*, *SIS*, *ECRIS-TCN*, kā arī Eiropola datos un Interpola datubāzēs;

b) drošs komunikāciju kanāls starp *ESP*, dalībvalstīm un Savienības aģentūrām, kurām ir tiesības izmantot *ESP*;

c) droša komunikāciju infrastruktūra starp *ESP* un IIS, VIS, *ETIAS*, *Eurodac*, centrālo *SIS*, *ECRIS-TCN*, Eiropola datiem un Interpola datubāzēm, kā arī starp *ESP* un *CIR* un *MID* centrālajām infrastruktūrām.

3. *eu-LISA* izstrādā *ESP* un nodrošina tā tehnisko pārvaldību.

7. pants

Eiropas meklēšanas portāla izmantošana

1. *ESP* izmantošana ir atļauta tikai dalībvalstu iestādēm un Savienības aģentūrām, kurām ir piekļuve vismaz vienai no ES informācijas sistēmām saskaņā ar tiesību instrumentiem, kas reglamentē minētās ES informācijas sistēmas, *CIR* un *MID* saskaņā ar šo regulu, Eiropola datiem saskaņā ar Regulu (ES) 2016/794 vai Interpola datubāzēm saskaņā ar Savienības vai valsts tiesību aktiem, kas reglamentē šādu piekļuvi.

Minētās dalībvalstu iestādes un Savienības aģentūras var izmantot *ESP* un tā sniegtos datus tikai tiem mērķiem un nolūkiem, kas ir paredzēti tiesību instrumentos, kuri reglamentē minētās ES informācijas sistēmas, Regulā (ES) 2016/794 un šajā regulā.

2. Šā panta 1. punktā minētās dalībvalstu iestādes un Savienības aģentūras izmanto *ESP*, lai saskaņā ar savām piekļuves tiesībām, kā minēts šo ES informācijas sistēmu reglamentējošos tiesību instrumentos un valsts tiesību aktos meklētu IIS, VIS un *ETIAS* centrālajās sistēmās ar personām vai viņu ceļošanas dokumentiem saistītus datus. Tās izmanto *ESP* arī, lai saskaņā ar to piekļuves tiesībām atbilstīgi šai regulai 20., 21. un 22. pantā minētajos nolūkos veiktu vaicājumus *CIR*.

3. Šā panta 1. punktā minētās dalībvalstu iestādes var izmantot *ESP*, lai centrālajā *SIS* meklētu ar personām vai viņu ceļošanas dokumentiem saistītus datus, kas minēti Regulās (ES) 2018/1860 un (ES) 2018/1861.

4. Ja to paredz Savienības tiesību akti, 1. punktā minētās Savienības aģentūras izmanto *ESP*, lai centrālajā *SIS* meklētu ar personām vai viņu ceļošanas dokumentiem saistītus datus.

5. Šā panta 1. punktā minētās dalībvalstu iestādes un Savienības aģentūras var izmantot *ESP*, lai saskaņā ar savām piekļuves tiesībām, ja tādas paredzētas Savienības un valsts tiesību aktos, meklētu Interpola datubāzēs ar ceļošanas dokumentiem saistītus datus.

8. pants

Eiropas meklēšanas portāla lietotāju profili

1. Lai varētu izmantot *ESP*, *eu-LISA* sadarbībā ar dalībvalstīm saskaņā ar 2. punktā minētajiem tehniskajiem parametriem un piekļuves tiesībām izveido profilu, kas balstīts uz katru *ESP* lietotāju kategoriju un uz vaicājumu nolūkiem. Katrs profils saskaņā ar Savienības un valsts tiesību aktiem ietver šādu informāciju:

a) vaicājumu veikšanai izmantojamos datu laukus;

b) ES informācijas sistēmas, Eiropola datus un Interpola datubāzes, kurās veicami vaicājumi, kurās var tikt veikti vaicājumi un kurām jāsniedz atbilde lietotājam;

c) konkrētos ES informācijas sistēmu, Eiropola datu un Interpola datubāzu datus, kuros var veikt vaicājumus;

d) datu kategorijas, kas var būt sniegti katrā atbildē.

2. Komisija pieņem īstenošanas aktus, lai precizētu 1. punktā minēto profilu tehniskos parametrus saskaņā ar *ESP* lietotāju piekļuves tiesībām atbilstīgi ES informācijas sistēmas reglamentējošiem tiesību instrumentiem un valsts tiesību aktiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

3. *eu-LISA* sadarbībā ar dalībvalstīm 1. punktā minētos profilus regulāri – vismaz reizi gadā – pārskata un vajadzības gadījumā atjaunina.

9. pants

Vaicājumi

1. *ESP* lietotāji veic vaicājumu, ievadot burtciparu vai biometriskos datus *ESP*. Ja vaicājums ir veikts, *ESP* ar lietotāja iesniegtajiem datiem un atbilstīgi lietotāja profilam vienlaikus veic vaicājumu IIS, *ETIAS*, VIS, *SIS*, *Eurodac*, *ECRIS-TCN*, *CIR*, Eiropola datos un Interpola datubāzēs.

2. Datu kategorijas, kuras izmanto, lai veiktu vaicājumu, izmantojot *ESP*, atbilst tām ar personām vai ceļošanas dokumentiem saistītajām datu kategorijām, kuras var izmantot, lai veiktu vaicājumus dažādās ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs saskaņā ar tos reglamentējošajiem tiesību instrumentiem.

3. *eu-LISA* sadarbībā ar dalībvalstīm ievieš saskarnes kontroldokumentu, kura pamatā ir 38. pantā minētais *UMF* attiecībā uz *ESP*.

4. Ja *ESP* lietotājs ir veicis vaicājumu, IIS, *ETIAS*, VIS, *SIS*, *Eurodac*, *ECRIS-TCN*, *CIR*, *MID*, Eiropola dati un Interpola datubāzes atbildē uz vaicājumu sniedz tajos esošos datus.

Neskarot 20. pantu, *ESP* sniegtajā atbildē norāda, kurai ES informācijas sistēmai vai datubāzei dati pieder.

ESP nesniedz informāciju par datiem ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs, kuriem lietotājam nav piekļuves atbilstīgi piemērojamiem Savienības un valsts tiesību aktiem.

5. Visus vaicājumus Interpola datubāzēs, kas veikti ar *ESP*, veic tā, ka Interpola brīdinājuma īpašniekam netiek atklāta nekāda informācija.

6. *ESP* atbildes lietotājam sniedz, tiklīdz ir pieejami dati no kādas ES informācijas sistēmas, Eiropola datiem vai Interpola datubāzēm. Minētajās atbildēs ietver tikai tādus datus, kuriem lietotājam ir piekļuve atbilstīgi Savienības un valsts tiesību aktiem.

7. Komisija pieņem īstenošanas aktu, lai precizētu tehnisko procedūru, kā *ESP* veic vaicājumus ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs, un *ESP* atbilžu formātu. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

10. pants

Reģistra ierakstu glabāšana

1. Neskarot Regulas (ES) 2017/2226 46. pantu, Regulas (EK) Nr. 767/2008 34. pantu, Regulas (ES) 2018/1240 69. pantu un Regulas (ES) 2018/1861 12. un 18. pantu, *eu-LISA* glabā reģistra ierakstus par visām *ESP* ietvaros veiktajām datu apstrādes darbībām. Minētie reģistra ieraksti satur šādu informāciju:

a) dalībvalsts iestāde vai Savienības aģentūra, kas veikusi vaicājumu, un izmantotais *ESP* profils;

b) vaicājuma datums un laiks;

c) ES informācijas sistēmas un Interpola datubāzes, kurās veikts vaicājums.

2. Katra dalībvalsts glabā reģistra ierakstus par vaicājumiem, ko veic tās iestādes un minēto iestāžu darbinieki, kuri ir pienācīgi pilnvaroti izmantot *ESP*. Katra Savienības aģentūra glabā reģistra ierakstus par vaicājumiem, ko veic tās pienācīgi pilnvaroti darbinieki.

3. Reģistra ierakstus, kas minēti 1. un 2. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām minētie reģistra ieraksti vairs nav vajadzīgi.

11. pants

Alternatīvās procedūras gadījumā, ja Eiropas meklēšanas portālu tehniski nav iespējams izmantot

1. Ja *ESP* nedarbošanās dēļ tehniski to nav iespējams izmantot, lai veiktu vaicājumu vienā vai vairākās ES informācijas sistēmās vai *CIR*, *eu-LISA* automatizēti informē *ESP* lietotājus.

2. Ja *ESP* tehniski nav iespējams izmantot, lai veiktu vaicājumu vienā vai vairākās ES informācijas sistēmās vai *CIR*, jo kādā dalībvalstī nedarbojas valsts infrastruktūra, minētā dalībvalsts automatizēti informē *eu-LISA* un Komisiju.

3. Šā panta 1. vai 2. punktā minētajos gadījumos – un līdz tehniskās kļūmes novēršanai – nepiemēro 7. panta 2. un 4. punktā minēto pienākumu un dalībvalstis tieši piekļūst ES informācijas sistēmām vai *CIR*, kad tas tām jādara atbilstīgi Savienības vai valsts tiesību aktiem.

4. Ja *ESP* tehniski nav iespējams izmantot, lai veiktu vaicājumu vienā vai vairākās ES informācijas sistēmās vai *CIR*, jo nedarbojas kādas Savienības aģentūras infrastruktūra, minētā aģentūra automatizēti informē *eu-LISA* un Komisiju.

III NODAĻA

Kopējs biometrisko datu salīdzināšanas pakalpojums

12. pants

Kopējs biometrisko datu salīdzināšanas pakalpojums

1. Tiek izveidots kopējs biometrisko datu salīdzināšanas pakalpojums (kopējais *BMS*), kas glabā biometriskās veidnes, kuras iegūtas no 13. pantā minētajiem *CIR* un *SIS* glabātajiem biometriskajiem datiem, un kas ļauj veikt biometrisko datu vaicājumus vairākās ES informācijas sistēmās, lai atbalstītu *CIR* un *MID* darbību un palīdzētu sasniegt IIS, VIS, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

2. Kopējo *BMS* veido:

a) centrāla infrastruktūra, kas aizstāj attiecīgi IIS, VIS, *SIS*, *Eurodac* un *ECRIS-TCN* centrālās sistēmas, ciktāl tā glabā biometriskās veidnes un dod iespēju meklēt ar biometriskajiem datiem;

b) droša komunikāciju infrastruktūra starp kopējo *BMS*, centrālo *SIS* un *CIR*.

3. *eu-LISA* izstrādā kopējo *BMS* un nodrošina tā tehnisko pārvaldību.

13. pants

Biometrisko veidņu glabāšana kopējā biometrisko datu salīdzināšanas pakalpojumā

1. Kopējā *BMS* glabā biometriskās veidnes, kuras tas iegūst no šādiem biometriskajiem datiem:

a) dati, kas minēti Regulas (ES) 2017/2226 16. panta 1. punkta d) apakšpunktā, 17. panta 1. punkta b) un c) apakšpunktā un 18. panta 2. punkta a), b) un c) apakšpunktā;

b) dati, kas minēti Regulas (EK) Nr. 767/2008 9. panta 6. punktā;

c) dati, kas minēti Regulas (ES) 2018/1861 20. panta 2. punkta w) un x) apakšpunktā, izņemot plaukstas nospiedumu datus;

d) dati, kas minēti Regulas (ES) 2018/1860 4. panta 1. punkta u) un v) apakšpunktā, izņemot plaukstas nospiedumu datus.

Biometriskās veidnes glabā kopējā *BMS* loģiski nodalītā veidā atbilstīgi ES informācijas sistēmai, no kuras dati ir iegūti.

2. Attiecībā uz katru 1. punktā minēto datu kopu kopējais *BMS* katrā biometriskajā veidnē ietver atsauci uz ES informācijas sistēmām, kurās atbilstošie biometriskie dati tiek glabāti, un atsauci uz faktiskajiem ierakstiem minētajās ES informācijas sistēmās.

3. Biometriskās veidnes tiek ievadītas kopējā *BMS* tikai pēc automatizētas vienai no ES informācijas sistēmām pievienoto biometrisko datu kvalitātes pārbaudes, ko veic kopējais *BMS*, lai pārliecinātos, ka ir ievēroti datu kvalitātes minimālie standarti.

4. Šā panta 1. punktā minēto datu glabāšana atbilst 37. panta 2. punktā minētajiem kvalitātes standartiem.

5. Komisija ar īstenošanas aktu nosaka veiktspējas prasības un praktisko kārtību, kā uzraudzīt kopējā *BMS* veiktspēju, lai nodrošinātu, ka biometrisko meklējumu efektivitāte ir pietiekama procedūrām, kurās ir izšķirīgs laiks, piemēram, robežpārbaudēm un identifikācijai. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

14. pants

Biometrisko datu meklēšana ar kopējā biometrisko datu salīdzināšanas pakalpojuma palīdzību

Lai meklētu *CIR* un *SIS* glabātos biometriskos datus, *CIR* un *SIS* izmanto biometriskās veidnes, kas tiek glabātas kopējā *BMS*. Vaicājumus ar biometriskajiem datiem veic saskaņā ar mērķiem, kas paredzēti šajā regulā un Regulās (EK) Nr. 767/2008, (ES) 2017/2226, (ES) 2018/1860, (ES) 2018/1861, (ES) 2018/1862 un (ES) 2019/816.

15. pants

Datu saglabāšana kopējā biometrisko datu salīdzināšanas pakalpojumā

Datus, kas minēti 13. panta 1. un 2. punktā, glabā kopējā *BMS* tikai tik ilgi, cik ilgi atbilstošos biometriskos datus glabā *CIR* vai *SIS*. Datu dzēšanu no kopējā *BMS* veic automatizēti.

16. pants

Reģistra ierakstu glabāšana

1. Neskarot Regulas (ES) 2017/2226 46. pantu, Regulas (EK) Nr. 767/2008 34. pantu un Regulas (ES) 2018/1861 12. un 18. pantu, *eu-LISA* glabā reģistra ierakstus par visām kopējā *BMS* ietvaros veiktajām datu apstrādes darbībām. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu;

b) vēsture, kas saistīta ar biometrisko veidņu izveidi un glabāšanu;

c) ES informācijas sistēmas, kurās veikti vaicājumi, izmantojot kopējā *BMS* glabātās biometriskās veidnes;

d) vaicājuma datums un laiks;

e) vaicājuma veikšanai izmantoto biometrisko datu veids;

f) vaicājuma rezultāti un rezultātu datums un laiks.

2. Katra dalībvalsts glabā reģistra ierakstus par tās iestāžu un minēto iestāžu darbinieku, kuri ir pienācīgi pilnvaroti izmantot kopējo *BMS*, veiktiem vaicājumiem. Katra Savienības aģentūra glabā reģistra ierakstus par tās pienācīgi pilnvarotu darbinieku veiktiem vaicājumiem.

3. Reģistra ierakstus, kas minēti 1. un 2. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām minētie reģistra ieraksti vairs nav vajadzīgi.

IV NODAĻA

Kopējs identitātes repozitorijs

17. pants

Kopējs identitātes repozitorijs

1. Tiek izveidots kopējs identitātes repozitorijs (*CIR*), ar kuru izveido individuālu personas datni par katru personu, kas reģistrēta IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, un kurā ir ietverti 18. pantā minētie dati, lai atvieglotu IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN* reģistrēto personu pareizu identifikāciju saskaņā ar 20. pantu, atbalstītu *MID* darbību saskaņā ar 21. pantu un atvieglotu un racionalizētu izraudzīto iestāžu un Eiropola piekļuvi IIS, VIS, *ETIAS* un *Eurodac*, ja tas vajadzīgs, lai novērstu, atklātu vai izmeklētu teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus saskaņā ar 22. pantu.

2. *CIR* veido:

a) centrāla infrastruktūra, kas aizstāj attiecīgi IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN* centrālās sistēmas, ciktāl tā glabā 18. pantā minētos datus;

b) drošs komunikāciju kanāls starp *CIR*, dalībvalstīm un Savienības aģentūrām, kurām ir tiesības izmantot *CIR* saskaņā ar Savienības un valsts tiesību aktiem;

c) droša komunikāciju infrastruktūra starp *CIR* un IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN*, kā arī ar *ESP*, kopējā *BMS* un *MID* centrālajām infrastruktūrām.

3. *eu-LISA* izstrādā *CIR* un nodrošina tā tehnisko pārvaldību.

4. Ja *CIR* tehnisku problēmu dēļ nav iespējams veikt vaicājumu *CIR*, lai identificētu personu saskaņā ar 20. pantu, konstatētu vairākas identitātes saskaņā ar 21. pantu vai novērstu, atklātu vai izmeklētu teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus saskaņā ar 22. pantu, *eu-LISA* automatizētā veidā informē *CIR* lietotājus.

5. *eu-LISA* sadarbībā ar dalībvalstīm ievieš saskarnes kontroldokumentu, kura pamatā ir 38. pantā minētais *UMF* attiecībā uz *CIR*.

18. pants

Kopējā identitātes repozitorija dati

1. *CIR* glabā šādus datus, kas loģiski nodalīti atbilstīgi tai informācijas sistēmai, no kuras dati tika iegūti:

a) dati, kas minēti Regulas (ES) 2017/2226 16. panta 1. punkta a) līdz d) apakšpunktā, 17. panta 1. punkta a), b) un c) apakšpunktā un 18. panta 1. un 2. punktā;

b) dati, kas minēti Regulas (EK) Nr. 767/2008 9. panta 4. punkta a) līdz c) apakšpunktā un 5. un 6. punktā;

c) dati, kas minēti Regulas (ES) Nr. 2018/1240 17. panta 2. punkta a) līdz e) apakšpunktā;

2. Attiecībā uz katru datu kopu, kas minēta 1. punktā, *CIR* ietver atsauci uz ES informācijas sistēmām, kurām dati pieder.

3. Iestādes, kas piekļūst *CIR*, to dara saskaņā ar to piekļuves tiesībām atbilstīgi ES informācijas sistēmas reglamentējošiem tiesību instrumentiem un valsts tiesību aktiem, un saskaņā ar to piekļuves tiesībām atbilstīgi šai regulai 20., 21. un 22. pantā minētajos nolūkos.

4. Attiecībā uz katru datu kopu, kas minēta 1. punktā, *CIR* ietver atsauci uz faktisko ierakstu ES informācijas sistēmās, kurām dati pieder.

5. Šā panta 1. punktā minēto datu glabāšana atbilst 37. panta 2. punktā minētajiem kvalitātes standartiem.

19. pants

Kopējā identitātes repozitorijā ietverto datu papildināšana, grozīšana un dzēšana

1. Ja IIS, VIS un *ETIAS* ietvertie dati tiek papildināti, grozīti vai dzēsti, tad 18. pantā minētos datus, kas glabājas *CIR* personas datnē, automatizētā veidā atbilstoši papildina, groza vai dzēš.

2. Ja *MID* saskaņā ar 32. vai 33. pantu ir izveidota balta vai sarkana saikne starp *CIR* veidojošo divu vai vairāku ES informācijas sistēmu datiem, *CIR* nevis izveido jaunu personas datni, bet pievieno jaunos datus ar saikni saistīto datu personas datnei.

20. pants

Piekļuve kopējam identitātes repozitorijam identifikācijas nolūkā

1. *CIR* vaicājumus veic policijas iestāde saskaņā ar 2. un 5. punktu tikai šādos apstākļos:

a) ja policijas iestāde nespēj identificēt personu, jo trūkst ceļošanas dokumenta vai cita ticama dokumenta, kas apliecinātu personas identitāti;

b) ja ir šaubas par attiecīgas personas sniegtajiem identitātes datiem;

c) ja ir šaubas par attiecīgas personas iesniegtā ceļošanas dokumenta vai cita ticama dokumenta autentiskumu;

d) ja ir šaubas par ceļošanas dokumenta vai cita ticama dokumenta turētāja identitāti; vai

e) ja persona nespēj vai atsakās sadarboties.

Šādi vaicājumi nav atļauti attiecībā uz nepilngadīgajiem, kas jaunāki par 12 gadiem, izņemot, ja tas ir bērna interesēs.

2. Ja iestājas kāds no 1. punktā minētajiem apstākļiem un policijas iestāde ir pilnvarota ar valsts leģislatīviem pasākumiem, kā minēts 5. punktā, tā – vienīgi personas identifikācijas nolūkos – var veikt vaicājumu *CIR*, izmantojot minētās personas biometriskos datus, kuri iegūti tiešā veidā identitātes pārbaudes laikā, ar noteikumu, ka šī procedūra sākta minētās personas klātbūtnē.

3. Ja vaicājuma rezultātā noskaidrojas, ka dati par minēto personu tiek glabāti *CIR*, policijas iestādei ir piekļuve aplūkot 18. panta 1. punktā minētos datus.

Ja personas biometriskie dati nav izmantojami vai ja vaicājums uz šo datu pamata neizdodas, vaicājumu veic, izmantojot personas identitātes datus apvienojumā ar ceļošanas dokumenta datiem, vai izmantojot identitātes datus, kurus sniegusi minētā persona.

4. Ja policijas iestāde ir pilnvarota ar valsts leģislatīviem pasākumiem, kā minēts 6. punktā, tā – vienīgi nolūkā identificēt nezināmas personas, kuras nespēj sevi identificēt, vai neidentificētas cilvēku mirstīgās atliekas dabas katastrofas, nelaimes gadījuma vai teroristu uzbrukuma gadījumā – var veikt vaicājumu *CIR*, izmantojot minēto personu biometriskos datus.

5. Dalībvalstis, kas vēlas izmantot 2. punktā paredzēto iespēju, pieņem valsts leģislatīvos pasākumus. To darot, dalībvalstis ņem vērā, ka ir jāizvairās no jebkādas trešo valstu valstspiederīgo diskriminācijas. Ar šādiem leģislatīviem pasākumiem konkretizē precīzos identifikācijas mērķus atbilstīgi 2. panta 1. punkta b) un c) apakšpunktā minētajiem mērķiem. Minētās dalībvalstis izraugās kompetentās policijas iestādes un nosaka šādu pārbaužu procedūras, nosacījumus un kritērijus.

6. Dalībvalstis, kas vēlas izmantot 4. punktā paredzēto iespēju, pieņem valsts leģislatīvos pasākumus, kuros noteiktas procedūras, nosacījumi un kritēriji.

21. pants

Piekļuve kopējam identitātes repozitorijam vairāku identitāšu konstatēšanas nolūkā

1. Ja *CIR* vaicājuma rezultāts ir dzeltena saikne atbilstoši 28. panta 4. punktam, tad iestādei, kas atbild par atšķirīgu identitāšu manuālu verifikāciju saskaņā ar 29. pantu, vienīgi šīs verifikācijas veikšanas nolūkā ir piekļuve 18. panta 1. un 2. punktā minētajiem *CIR* glabātajiem datiem, kuri ir saistīti ar dzeltenu saikni.

2. Ja *CIR* vaicājuma rezultāts ir sarkana saikne atbilstoši 32. pantam, tad 26. panta 2. punktā minētajām iestādēm vienīgi identitātes viltošanas apkarošanas nolūkos ir piekļuve 18. panta 1. un 2. punktā minētajiem *CIR* glabātajiem datiem, kuri ir saistīti ar sarkanu saikni.

22. pants

Vaicājumi kopējā identitātes repozitorijā nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus

1. Ja kādā konkrētā lietā ir pamatots iemesls uzskatīt, ka ES informācijas sistēmu aplūkošana palīdzēs novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, jo īpaši tad, ja ir aizdomas, ka teroristu nodarījumā vai citos smagos noziedzīgos nodarījumos aizdomās turamais, vainīgais vai cietušais ir persona, kuras dati tiek glabāti IIS, VIS vai *ETIAS*, izraudzītās iestādes un Eiropols var aplūkot *CIR*, lai iegūtu informāciju, vai dati par konkrētu personu atrodas IIS, VIS vai *ETIAS*.

2. Ja atbildē uz vaicājumu *CIR* norāda, ka dati par minēto personu atrodas IIS, VIS vai *ETIAS*, *CIR* sniedz izraudzītajām iestādēm un Eiropolam atbildi atsauces veidā, kā minēts 18. panta 2. punktā, norādot, kurā no minētajām ES informācijas sistēmām ir ietverti vaicājumam atbilstīgie dati. *CIR* atbild tā, lai netiktu apdraudēta datu drošība.

Atbildi, kurā ir norādīts, ka dati par minēto personu ir atrodami kādā no 1. punktā minētajām ES informācijas sistēmām, izmanto tikai pilnīgas piekļuves pieprasījuma iesniegšanas nolūkiem, ievērojot nosacījumus un procedūras, kas ir noteiktas attiecīgajos tiesību instrumentos, kuri reglamentē šādu piekļuvi.

Atbilstības vai vairāku atbilstību gadījumā izraudzītā iestāde vai Eiropols pieprasa pilnīgu piekļuvi vismaz vienai no informācijas sistēmām, no kuras tika ģenerēta atbilstība.

Ja izņēmuma gadījumā šāda pilnīga piekļuve netiek pieprasīta, izraudzītās iestādes reģistrē pamatojumu pieprasījuma neveikšanai, kas ir izsekojams līdz valsts datnei. Eiropols reģistrē pamatojumu attiecīgajā datnē.

3. Pilnīga piekļuve IIS,VIS vai *ETIAS* ietvertajiem datiem nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus joprojām ir pakļauta nosacījumiem un procedūrām, kas izklāstīti attiecīgajos tiesību instrumentos, kuri reglamentē šādu piekļuvi.

23. pants

Datu saglabāšana kopējā identitātes repozitorijā

1. Datus, kas minēti 18. panta 1., 2. un 4. punktā, automatizētā veidā dzēš no *CIR* saskaņā ar datu saglabāšanas noteikumiem, kuri attiecīgi paredzēti Regulās (ES) 2017/2226, (EK) Nr. 767/2008 un (ES) 2018/1240.

2. Personas datni glabā *CIR* tikai tik ilgi, cik ilgi atbilstošie dati tiek glabāti vismaz vienā no ES informācijas sistēmām, kuru dati ir ietverti *CIR*. Saiknes izveide neietekmē katra saistīto datu elementa saglabāšanas periodu.

24. pants

Reģistra ierakstu glabāšana

1. Neskarot Regulas (ES) 2017/2226 46. pantu, Regulas (EK) Nr. 767/2008 34. pantu un Regulas (ES) 2018/1240 69. pantu, *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām saskaņā ar šā panta 2., 3. un 4. punktu.

2. *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām, ievērojot 20. pantu. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu;

b) tā lietotāja piekļuves nolūks, kurš veic vaicājumu ar *CIR* starpniecību;

c) vaicājuma datums un laiks;

d) vaicājuma veikšanai izmantoto datu veids;

e) vaicājuma rezultāti.

3. *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām, ievērojot 21. pantu. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu;

b) tā lietotāja piekļuves nolūks, kurš veic vaicājumu ar *CIR* starpniecību;

c) vaicājuma datums un laiks;

d) ja ir izveidota saikne – vaicājuma veikšanai izmantotie dati un vaicājuma rezultāti, norādot ES informācijas sistēmu, no kuras dati tika saņemti.

4. *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām, ievērojot 22. pantu. Minētie reģistra ieraksti ietver šādu informāciju:

a) vaicājuma datums un laiks;

b) vaicājuma veikšanai izmantotie dati;

c) vaicājuma rezultāti;

d) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu *CIR*.

Kompetentā uzraudzības iestāde saskaņā ar Direktīvas (ES) 2016/680 41. pantu vai Eiropas Datu aizsardzības uzraudzītājs saskaņā ar Regulas (ES) 2016/794 43. pantu ne retāk kā reizi sešos mēnešos regulāri verificē reģistra ierakstus par šādu piekļuvi, lai pārbaudītu, vai ir ievērotas šīs regulas 22. panta 1. un 2. punktā noteiktās procedūras un nosacījumi.

5. Katra dalībvalsts glabā reģistra ierakstus par vaicājumiem, ko tās iestādes un minēto iestāžu darbinieki, kuri ir pienācīgi pilnvaroti izmantot *CIR*, veic saskaņā ar 20., 21. un 22. pantu. Katra Savienības aģentūra glabā reģistra ierakstus par vaicājumiem, ko tās pienācīgi pilnvaroti darbinieki veic saskaņā ar 21. un 22. pantu.

Papildus tam attiecībā uz jebkādu piekļuvi *CIR* saskaņā ar 22. pantu katra dalībvalsts glabā šādus reģistra ierakstus:

a) atsauce uz valsts datni;

b) piekļuves nolūks;

c) saskaņā ar valsts noteikumiem – tās amatpersonas unikālā lietotāja identitāte, kura veica vaicājumu, un tās amatpersonas unikālā lietotāja identitāte, kura lika veikt vaicājumu.

6. Saskaņā ar Regulu (ES) 2016/794 Eiropols par jebkādu piekļuvi *CIR*, ko piešķir atbilstoši šīs regulas 22. pantam, glabā reģistra ierakstus par tās amatpersonas unikālo lietotāja identitāti, kura veica vaicājumu, un tās amatpersonas unikālo lietotāja identitāti, kura lika veikt vaicājumu.

7. Reģistra ierakstus, kas minēti 2. līdz 6. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām minētie reģistra ieraksti vairs nav vajadzīgi.

8. *eu-LISA* glabā reģistra ierakstus, kas saistīti ar personas datnēs glabāto datu vēsturi. *eu-LISA* šādus reģistra ierakstus automatizēti dzēš, kolīdz dati ir dzēsti.

V NODAĻA

Vairāku identitāšu detektors

25. pants

Vairāku identitāšu detektors

1. Tiek izveidots vairāku identitāšu detektors (*MID*), ar kuru izveido un glabā 34. pantā minētās identitātes apstiprinājuma datnes, kas satur saiknes starp datiem ES informācijas sistēmās, kuras ir iekļautas *CIR* un *SIS* un kas ļauj konstatēt vairākas identitātes, nolūkā sasniegt divējādu mērķi, proti, atvieglot identitātes pārbaudes un apkarot identitātes viltošanu, lai atbalstītu *CIR* darbību un palīdzētu sasniegt IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

2. *MID* veido:

a) centrāla infrastruktūra, kas glabā saiknes un atsauces uz ES informācijas sistēmām;

b) droša komunikāciju infrastruktūra, kuras mērķis ir savienot *MID* ar *SIS* un centrālajām *ESP* un *CIR* infrastruktūrām.

3. *eu-LISA* izstrādā *MID* un nodrošina tā tehnisko pārvaldību.

26. pants

Piekļuve vairāku identitāšu detektoram

1. Lai veiktu atšķirīgu identitāšu manuālu verifikāciju, kas minēta 29. pantā, piekļuvi 34. pantā minētajiem datiem, kas tiek glabāti *MID*, piešķir:

a) saskaņā ar Regulas (ES) 2017/2226 9. panta 2. punktu izraudzītajām kompetentajām iestādēm, kad IIS izveido vai atjaunina individuālu personas datni saskaņā ar minētās regulas 14. pantu;

b) Regulas (EK) Nr. 767/2008 6. panta 1. punktā minētajām vīzu iestādēm, kad VIS izveido vai atjaunina pieteikuma datni saskaņā ar minēto regulu;

c) *ETIAS* centrālajai vienībai un *ETIAS* valsts vienībām, kad veic Regulas (ES) 2018/1240 22. un 26. pantā minēto apstrādi;

d) tās dalībvalsts *SIRENE* birojam, kura izveido vai atjaunina *SIS* brīdinājumu saskaņā ar Regulu (ES) 2018/1860 un Regulu (ES) 2018/1861.

2. Dalībvalsts iestādēm un Savienības aģentūrām, kurām ir piekļuve vismaz vienai *CIR* iekļautajai ES informācijas sistēmai vai kurām ir piekļuve *SIS*, ir piekļuve 34. panta a) un b) punktā minētajiem datiem attiecībā uz jebkādu sarkanu saikni, kas minēta 32. pantā.

3. Dalībvalstu iestādēm un Savienības aģentūrām ir piekļuve baltajām saiknēm, kas minētas 33. pantā, ja tām ir piekļuve abām ES informācijas sistēmām, kurās ir dati, starp kuriem izveidota baltā saikne.

4. Dalībvalstu iestādēm un Savienības aģentūrām ir piekļuve zaļajām saiknēm, kas minētas 31. pantā, ja tām ir piekļuve abām ES informācijas sistēmām, kurās ir dati, starp kuriem izveidota zaļā saikne, un vaicājums šajās informācijas sistēmās ir atklājis atbilstību attiecībā pret abām saistīto datu kopām.

27. pants

Vairāku identitāšu konstatēšana

1. *CIR* un *SIS* veic vairāku identitāšu konstatēšanu, ja:

a) IIS saskaņā ar Regulas (ES) 2017/226 14. pantu ir izveidota vai atjaunināta personas datne;

b) VIS saskaņā ar Regulu (EK) Nr. 767/2008 ir izveidota vai atjaunināta pieteikuma datne;

c) *ETIAS* sistēmā saskaņā ar Regulas (ES) 2018/1240 19. pantu ir izveidota vai atjaunināta pieteikuma datne;

d) *SIS* ir izveidots vai atjaunināts brīdinājums par personu saskaņā ar Regulas (ES) 2018/1860 3. pantu un Regulas (ES) 2018/1861 V nodaļu.

2. Ja datos, kas ietverti kādā no 1. punktā minētajām ES informācijas sistēmām, ir biometriskie dati, tad *CIR* un centrālā *SIS* izmanto kopējo *BMS*, lai veiktu vairāku identitāšu konstatēšanu. Kopējais *BMS* salīdzina no jebkādiem jauniem biometriskiem datiem iegūtās biometriskās veidnes ar kopējā *BMS* jau ietvertajām biometriskajām veidnēm, lai pārbaudītu, vai dati, kas attiecas uz vienu un to pašu personu, jau tiek glabāti *CIR* vai centrālajā *SIS*.

3. Papildus 2. punktā minētajam procesam *CIR* un centrālā *SIS* izmanto *ESP*, lai meklētu attiecīgi *CIR* un centrālajā *SIS* glabātos datus, izmantojot šādus datus:

a) uzvārds; vārds vai vārdi; dzimšanas datums, valstspiederība vai valstspiederības; un dzimums, kā minēts Regulas (ES) 2017/2226 16. panta 1. punkta a) apakšpunktā, 17. panta 1. punktā un 18. panta 1. punktā;

b) uzvārds; vārds vai vārdi; dzimšanas datums; dzimums; dzimšanas vieta un valsts; un valstspiederības, kā minēts Regulas (EK) Nr. 767/2008 9. panta 4. punkta a) un aa) apakšpunktā;

c) uzvārds; vārds(-i); uzvārds dzimšanas brīdī; pseidonīmi; dzimšanas datums, dzimšanas vieta, dzimums un pašreizējā valstspiederība, kā minēts Regulas (ES) 2018/1240 17. panta 2. punktā;

d) uzvārdi; vārdi; vārdi, uzvārdi dzimšanas brīdī, iepriekš lietoti vārdi un pseidonīmi; dzimšanas vieta, dzimšanas datums, dzimums un visas valstspiederības, kā minēts Regulas (ES) 2018/1861 20. panta 2. punktā.

e) uzvārdi; vārdi; vārdi, uzvārdi dzimšanas brīdī; iepriekš lietoti vārdi un pseidonīmi; dzimšanas vieta, dzimšanas datums; dzimums; un visas valstspiederības, kā minēts Regulas (ES) 2018/1860 4. pantā.

4. Papildus 2. un 3. punktā minētajam procesam *CIR* un centrālā *SIS* izmanto *ESP*, lai meklētu attiecīgi centrālajā *SIS* un *CIR* glabātos datus, izmantojot ceļošanas dokumenta datus.

5. Vairāku identitāšu konstatēšanu veic vienīgi, lai salīdzinātu vienā ES informācijas sistēmā pieejamos datus ar datiem, kas pieejami citās ES informācijas sistēmās.

28. pants

Vairāku identitāšu konstatēšanas rezultāti

1. Ja 27. panta 2., 3. un 4. punktā minētie vaicājumi neuzrāda nevienu atbilstību, tad turpina 27. panta 1. punktā minētās procedūras saskaņā ar tās reglamentējošiem tiesību instrumentiem.

2. Ja 27. panta 2., 3. un 4. punktā minētais vaicājums uzrāda vienu vai vairākas atbilstības, tad *CIR* un – vajadzības gadījumā – *SIS* izveido saikni starp vaicājuma veikšanai izmantotajiem datiem un datiem, uz kuriem attiecas atbilstība.

Ja tiek uzrādītas vairākas atbilstības, izveido saikni starp visiem datiem, uz kuriem attiecas atbilstība. Ja dati jau bija saistīti, esošo saikni paplašina, ietverot arī vaicājuma veikšanai izmantotos datus.

3. Ja 27. panta 2., 3. un 4. punktā minētais vaicājums uzrāda vienu vai vairākas atbilstības un saistīto datņu identitātes dati ir tādi paši vai līdzīgi, tad izveido baltu saikni saskaņā ar 33. pantu.

4. Ja 27. panta 2., 3. un 4. punktā minētais vaicājums uzrāda vienu vai vairākas atbilstības un saistīto datņu identitātes datus nevar uzskatīt par līdzīgiem, tad izveido dzeltenu saikni saskaņā ar 30. pantu un piemēro 29. pantā minēto procedūru.

5. Komisija pieņem deleģētos aktus saskaņā ar 73. pantu, paredzot procedūras tādu gadījumu noteikšanai, kuros identitātes datus var uzskatīt par tādiem pašiem vai līdzīgiem.

6. Saiknes glabā 34. pantā minētajā identitātes apstiprinājuma datnē.

7. Komisija sadarbībā ar *eu-LISA* ar īstenošanas aktiem nosaka tehniskos noteikumus saikņu izveidošanai starp datiem no dažādām ES informācijas sistēmām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

29. pants

Atšķirīgu identitāšu manuāla verifikācija un atbildīgās iestādes

1. Neskarot 2. punktu, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir:

a) kompetentā iestāde, kas izraudzīta saskaņā ar Regulas (ES) 2017/2226 9. panta 2. punktu, attiecībā uz atbilstībām, kas tika uzrādītas brīdī, kad IIS saskaņā ar minēto regulu tika izveidota vai atjaunināta personas datne;

b) Regulas (EK) Nr. 767/2008 6. panta 1. punktā minētās vīzu iestādes attiecībā uz atbilstībām, kas tika uzrādītas brīdī, kad VIS tika izveidota vai atjaunināta pieteikuma datne saskaņā ar minēto Regulu;

c) *ETIAS* centrālā vienība un *ETIAS* valsts vienības attiecībā uz atbilstībām, kas tika uzrādītas brīdī, kad tika izveidota vai atjaunināta pieteikuma datne saskaņā ar Regulu (ES) 2018/1240;

d) dalībvalsts *SIRENE* birojs attiecībā uz atbilstībām, kas tika uzrādītas brīdī, kad tika izveidots vai atjaunināts *SIS* brīdinājums saskaņā ar Regulu (ES) 2018/1860 un Regulu (ES) 2018/1861.

MID norāda iestādi, kas ir atbildīga par atšķirīgu identitāšu manuālu verifikāciju, identitātes apstiprinājuma datnē.

2. Par atšķirīgu identitāšu manuālu verifikāciju identitātes apstiprinājuma datnē atbildīgā iestāde ir brīdinājumu izveidojušās dalībvalsts *SIRENE* birojs, ja ir izveidota saikne uz datiem, kas ir ietverti brīdinājumā par:

a) personām, ko meklē, lai apcietinātu nolūkā tās nodot vai izdot, kā minēts Regulas (ES) 2018/1862 26. pantā;

b) pazudušām personām vai neaizsargātām personām, kā minēts Regulas (ES) 2018/1862 32. pantā;

c) personām, ko cenšas atrast, lai tās varētu palīdzēt tiesas procesā, kā minēts Regulas (ES) 2018/1862 34. pantā;

d) personām diskrētu pārbaužu, izmeklēšanas pārbaužu vai īpašu pārbaužu vajadzībām, kā minēts Regulas (ES) 2018/1862 36. pantā.

3. Neskarot šā panta 4. punktu, par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai iestādei ir piekļuve saistītajiem datiem, kas ietverti attiecīgajā identitātes apstiprinājuma datnē, un identitātes datiem, uz kuriem ir saikne *CIR* un – vajadzības gadījumā – *SIS*. Tā novērtē atšķirīgās identitātes nekavējoties. Tiklīdz novērtēšana ir pabeigta, tā atjaunina saikni saskaņā ar 31., 32. un 33. pantu un nekavējoties pievieno to identitātes apstiprinājuma datnei.

4. Ja par atšķirīgu identitāšu manuālu verifikāciju identitātes apstiprinājuma datnē atbildīgā iestāde ir kompetentā iestāde, kura izraudzīta saskaņā ar Regulas (ES) 2017/2226 9. panta 2. punktu un kura IIS izveido vai atjaunina personas datni saskaņā ar minētās regulas 14. pantu, un ja ir izveidota dzeltena saikne, tad minētā iestāde veic papildu pārbaudes. Minētajai iestādei tikai un vienīgi minētajā nolūkā ir piekļuve saistītajiem datiem, kas ietverti attiecīgajā identitātes apstiprinājuma datnē. Tā novērtē atšķirīgās identitātes un atjaunina saikni saskaņā ar šīs regulas 31., 32. un 33. pantu, un nekavējoties pievieno to identitātes apstiprinājuma datnei.

Šāda atšķirīgu identitāšu manuāla verifikācija vienmēr tiek sākta attiecīgās personas klātbūtnē, un šai personai piedāvā iespēju paskaidrot apstākļus atbildīgajai iestādei, kura šos paskaidrojumus ņem vērā.

Gadījumos, kad atšķirīgu identitāšu manuāla verifikācija notiek uz robežas, to, ja iespējams, veic 12 stundu laikā pēc dzeltenās saiknes izveides saskaņā ar 28. panta 4. punktu.

5. Ja ir izveidota vairāk nekā viena saikne, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde katru saikni izvērtē atsevišķi.

6. Ja dati, uz kuru pamata ir uzrādīta atbilstība, jau bija saistīti, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ņem vērā esošās saiknes, izvērtējot jaunu saikņu izveidi.

30. pants

Dzeltena saikne

1. Ja atšķirīgu identitāšu manuāla verifikācija vēl nav veikta, saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā dzeltenu jebkurā no šādiem gadījumiem:

a) saistītajos datos ir vieni un tie paši biometriskie dati, bet ir līdzīgi vai atšķirīgi identitātes dati;

b) saistītajos datos ir atšķirīgi identitātes dati, bet ir vieni un tie paši ceļošanas dokumenta dati, un vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu;

c) saistītajos datos ir vieni un tie paši identitātes dati, bet ir atšķirīgi biometriskie dati;

d) saistītajos datos ir līdzīgi vai atšķirīgi identitātes dati un ir vieni un tie paši ceļošanas dokumenta dati, bet ir atšķirīgi biometriskie dati.

2. Ja saikne ir klasificēta kā dzeltena saskaņā ar 1. punktu, piemēro 29. pantā noteikto procedūru.

31. pants

Zaļa saikne

1. Saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā zaļu, ja:

a) saistītajos datos ir atšķirīgi biometriskie dati, bet ir vieni un tie paši identitātes dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām;

b) saistītajos datos ir atšķirīgi biometriskie dati, ir līdzīgi vai atšķirīgi identitātes dati, ir vieni un tie paši ceļošanas dokumenta dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām;

c) saistītajos datos ir atšķirīgi identitātes dati, bet ir vieni un tie paši ceļošanas dokumenta dati, vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām.

2. Ja veic vaicājumu *CIR* vai *SIS* un ja pastāv zaļa saikne starp datiem divās vai vairākās ES informācijas sistēmās, *MID* norāda, ka saistīto datu identitātes dati neatbilst vienai un tai pašai personai.

3. Ja dalībvalsts iestādei ir pierādījumi, ka zaļā saikne ir nepareizi reģistrēta *MID*, ka zaļā saikne nav atjaunināta vai ka dati ir apstrādāti *MID* vai ES informācijas sistēmās, pārkāpjot šo regulu, tā pārbauda attiecīgos datus, kas glabājas *CIR* un *SIS*, un vajadzības gadījumā nekavējoties izlabo vai dzēš saikni no *MID*. Minētā dalībvalsts iestāde nekavējoties informē dalībvalsti, kas ir atbildīga par atšķirīgu identitāšu manuālu verifikāciju.

32. pants

Sarkana saikne

1. Saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā sarkanu jebkurā no šādiem gadījumiem:

a) saistītajos datos ir vieni un tie paši biometriskie dati, bet ir līdzīgi vai atšķirīgi identitātes dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati nepamatoti attiecas uz vienu un to pašu personu;

b) saistītajos datos ir vieni un tie paši, līdzīgi vai atšķirīgi identitātes dati un vieni un tie paši ceļošanas dokumenta dati, bet atšķirīgi biometriskie dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām, no kurām vismaz viena nepamatoti izmanto vienu un to pašu ceļošanas dokumentu;

c) saistītajos datos ir vieni un tie paši identitātes dati, bet ir atšķirīgi biometriskie dati un atšķirīgi ceļošanas dokumenta dati – vai tādu nemaz nav –, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati nepamatoti attiecas uz divām dažādām personām;

d) saistītajos datos ir atšķirīgi identitātes dati, bet ir vieni un tie paši ceļošanas dokumenta dati, vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati nepamatoti attiecas uz vienu un to pašu personu.

2. Ja veic vaicājumu *CIR* vai *SIS* un pastāv sarkana saikne starp datiem divās vai vairākās ES informācijas sistēmās, *MID* norāda 34. pantā minētos datus. Turpmākos pasākumus sarkanas saiknes gadījumā veic saskaņā ar Savienības un valsts tiesību aktiem, jebkādas juridiskās sekas attiecīgajai personai balstot tikai uz atbilstīgajiem datiem par minēto personu. Tikai sarkanas saiknes pastāvēšana vien nerada attiecīgajai personai nekādas juridiskas sekas.

3. Ja ir izveidota sarkana saikne starp datiem no IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, *CIR* glabāto personas datni atjaunina saskaņā ar 19. panta 2. punktu.

4. Neskarot Regulās (ES) 2018/1860, (ES) 2018/1861 un (ES) 2018/1862 minētos noteikumus par brīdinājumu apstrādi *SIS* un neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību un sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta nekāda valsts veikta izmeklēšana, gadījumos, kad ir izveidota sarkana saikne, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde informē attiecīgo personu par vairāku nelikumīgu identitātes datu esamību un sniedz personai vienotu identifikācijas numuru, kas minēts šīs regulas 34. panta c) punktā, atsauci uz iestādi, kas atbild par atšķirīgu identitāšu manuālu verifikāciju un minēta šīs regulas 34. panta d) punktā, un saskaņā ar šīs regulas 49. pantu izveidotā tīmekļa portāla tīmekļa adresi.

5. Par atšķirīgo identitāšu manuālu verifikāciju atbildīgā iestāde sniedz 4. punktā minēto informāciju rakstveidā standarta veidlapā. Komisija ar īstenošanas aktiem nosaka minētās veidlapas saturu un izklāstu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

6. Ja ir izveidota sarkana saikne, *MID* automatizēti informē iestādes, kas atbild par saistītajiem datiem.

7. Ja dalībvalsts iestādei vai Savienības aģentūrai, kurai ir piekļuve *CIR* vai *SIS*, ir pierādījumi, kas liecina, ka sarkana saikne ir nepareizi reģistrēta *MID* vai ka *MID*, *CIR* vai *SIS* dati ir apstrādāti, pārkāpjot šo regulu, minētā iestāde vai aģentūra pārbauda attiecīgos *CIR* vai *SIS* glabātos datus un:

a) ja saikne attiecas uz kādu no 29. panta 2. punktā minētajiem *SIS* brīdinājumiem, nekavējoties informē tās dalībvalsts attiecīgo *SIRENE* biroju, kura izveidojusi minēto *SIS* brīdinājumu.

b) visos citos gadījumos nekavējoties labo vai dzēš saikni no *MID*.

Ja ar *SIRENE* biroju sazinās, ievērojot pirmās daļas a) punktu, tas pārbauda dalībvalsts iestādes vai Savienības aģentūras sniegtos pierādījumus un attiecīgā gadījumā nekavējoties labo vai dzēš saikni no *MID*.

Dalībvalsts iestāde, kas ieguvusi pierādījumus, nekavējoties informē par atšķirīgu identitāšu manuālu verifikāciju atbildīgo dalībvalsts iestādi par jebkuru attiecīgu sarkanas saiknes labošanu vai dzēšanu.

33. pants

Balta saikne

1. Saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā baltu jebkurā no šādiem gadījumiem:

a) saistītajos datos ir vieni un tie paši biometriskie dati un vieni un tie paši vai līdzīgi identitātes dati;

b) saistītajos datos ir vieni un tie paši vai līdzīgi identitātes dati, vieni un tie paši ceļošanas dokumenta dati, un vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu;

c) saistītajos datos ir vieni un tie paši biometriskie dati, vieni un tie paši ceļošanas dokumenta dati un līdzīgi identitātes dati;

d) saistītajos datos ir vieni un tie paši biometriskie dati, bet ir līdzīgi vai atšķirīgi identitātes dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati pamatoti attiecas uz vienu un to pašu personu.

2. Ja veic vaicājumu *CIR* vai *SIS* un pastāv balta saikne starp datiem divās vai vairākās ES informācijas sistēmās, *MID* norāda, ka saistīto datu identitātes dati atbilst vienai un tai pašai personai. ES informācijas sistēmas, kurās veikts vaicājums, sniedz atbildi, vajadzības gadījumā norādot visus saistītos datus par personu, tādējādi izraisot atbilstību datiem, kas saistīti ar balto saikni, ja vaicājumu veicošajai iestādei saskaņā ar Savienības vai valsts tiesību aktiem ir piekļuve saistītajiem datiem.

3. Ja ir izveidota balta saikne starp datiem no IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, *CIR* glabāto personas datni atjaunina saskaņā ar 19. panta 2. punktu.

4. Neskarot Regulās (ES) 2018/1860, (ES) 2018/1861 un (ES) 2018/1862 minētos noteikumus par brīdinājumu apstrādi *SIS* un neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību un sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta valsts veikta izmeklēšana, gadījumos, kad pēc atšķirīgu identitāšu manuālas verifikācijas ir izveidota balta saikne, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde informē attiecīgo personu par līdzīgu vai atšķirīgu identitātes datu esamību un sniedz personai vienotu identifikācijas numuru, kā minēts šīs regulas 34. panta c) punktā, atsauci uz iestādi, kas atbild par atšķirīgo identitāšu manuālu verifikāciju, kā minēts šīs regulas 34. panta d) punktā, un saskaņā ar šīs regulas 49. pantu izveidotā tīmekļa portāla tīmekļa adresi.

5. Ja kādas dalībvalsts iestādes rīcībā ir pierādījumi, ka baltā saikne ir nepareizi reģistrēta *MID*, ka baltā saikne nav atjaunināta vai ka dati ir apstrādāti *MID* vai ES informācijas sistēmās, pārkāpjot šo regulu, tā pārbauda attiecīgos datus, kas glabājas *CIR* un *SIS*, un vajadzības gadījumā nekavējoties labo vai dzēš saikni no *MID*. Minētā dalībvalsts iestāde nekavējoties informē dalībvalsti, kas atbildīga par atšķirīgu identitāšu manuālu verifikāciju.

6. Iestāde, kas atbildīga par atšķirīgu identitāšu manuālu verifikāciju, sniedz 4. punktā minēto informāciju rakstveidā standarta veidlapā. Komisija ar īstenošanas aktiem nosaka minētās veidlapas saturu un izklāstu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

34. pants

Identitātes apstiprinājuma datne

Identitātes apstiprinājuma datnē ir iekļauti šādi dati:

a) saiknes, kas minētas 30. līdz 33. pantā;

b) atsauce uz ES informācijas sistēmām, kurās ir saistītie dati;

c) vienots identifikācijas numurs, kas ļauj izgūt saistītos datus no atbilstošajām ES informācijas sistēmām;

d) iestāde, kas atbild par atšķirīgu identitāšu manuālu verifikāciju;

e) saiknes izveides vai atjaunināšanas datums.

35. pants

Datu saglabāšana vairāku identitāšu detektorā

Identitātes apstiprinājuma datnes un tajās esošos datus, tostarp saiknes, glabā *MID* tikai tik ilgi, kamēr saistītie dati tiek glabāti divās vai vairākās ES informācijas sistēmās. To dzēšanu no *MID* veic automatizēti.

36. pants

Reģistra ierakstu glabāšana

1. *eu-LISA* glabā reģistra ierakstus par visām *MID* veiktajām datu apstrādes darbībām. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts, kas uzsāk meklēšanu;

b) lietotāja piekļuves nolūks;

c) vaicājuma datums un laiks;

d) vaicājuma vai vaicājumu veikšanai izmantoto datu veids;

e) atsauce uz saistītajiem datiem;

f) identitātes apstiprinājuma datnes vēsture.

2. Katra dalībvalsts glabā reģistra ierakstus par vaicājumiem, ko veic to iestādes un minēto iestāžu darbinieki, kuri ir pienācīgi pilnvaroti izmantot *MID*. Katra Savienības aģentūra glabā reģistra ierakstus par vaicājumiem, ko veic tās darbinieki, kuri ir pienācīgi pilnvaroti.

3. Reģistra ierakstus, kas minēti 1. un 2. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām reģistra ieraksti vairs nav vajadzīgi.

VI NODAĻA

Pasākumi sadarbspējas atbalstam

37. pants

Datu kvalitāte

1. Neskarot dalībvalstu pienākumus attiecībā uz sistēmās ievadīto datu kvalitāti, *eu-LISA* izveido automatizētus datu kvalitātes kontroles mehānismus un procedūras attiecībā uz datiem, kas glabāti IIS, VIS, *ETIAS*, *SIS*, kopējā *BMS* un *CIR*.

2. *eu-LISA* īsteno mehānismus kopējā *BMS* precizitātes novērtēšanai, kopējus datu kvalitātes indikatorus un minimālos kvalitātes standartus datu glabāšanai IIS, VIS, *ETIAS*, *SIS*, kopējā *BMS* un *CIR*.

IIS, VIS, *ETIAS*, VIS, *SIS*, kopējā *BMS*, *CIR* un *MID* var ievadīt tikai tādus datus, kas atbilst minimālajiem kvalitātes standartiem.

3. *eu-LISA* regulāri sniedz dalībvalstīm ziņojumus par automatizētajiem datu kvalitātes kontroles mehānismiem un procedūrām un kopējiem datu kvalitātes indikatoriem. *eu-LISA* arī regulāri sniedz Komisijai ziņojumus par jautājumiem, ar ko tā saskārusies, un dalībvalstīm, kurus tie skar. *eu-LISA* šādu ziņojumu pēc pieprasījuma iesniedz arī Eiropas Parlamentam un Padomei. Nevienā ziņojumā, kuru izstrādā saskaņā ar šo punktu, nedrīkst būt personas dati.

4. Īstenošanas aktos paredz sīki izstrādātus noteikumus – jo īpaši attiecībā uz biometriskajiem datiem – par automatizētajiem datu kvalitātes kontroles mehānismiem un procedūrām, kopējiem datu kvalitātes indikatoriem un minimālajiem kvalitātes standartiem datu glabāšanai IIS, VIS, *ETIAS*, *SIS*, kopējā *BMS* un *CIR*. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

5. Vienu gadu pēc automatizēto datu kvalitātes kontroles mehānismu un procedūru, kopējo datu kvalitātes indikatoru un datu minimālo kvalitātes standartu izveides un turpmāk ik gadu Komisija izvērtē datu kvalitātes īstenošanu dalībvalstīs un sniedz jebkādus nepieciešamos ieteikumus. Dalībvalstis iesniedz Komisijai rīcības plānu par to, kā novērst visus izvērtēšanas ziņojumā konstatētos trūkumus, un jo īpaši par datu kvalitātes problēmām, kas radušās no kļūdainiem datiem ES informācijas sistēmās. Dalībvalstis regulāri ziņo Komisijai par šā rīcības plāna īstenošanā panākto progresu tik ilgi, kamēr tas ir pilnībā īstenots.

Komisija izvērtēšanas ziņojumu nosūta Eiropas Parlamentam, Padomei, Eiropas Datu aizsardzības uzraudzītājam, Eiropas Datu aizsardzības kolēģijai un Eiropas Savienības Pamattiesību aģentūrai, kas izveidota ar Padomes Regulu (EK) Nr. 168/2007 ([39]).

38. pants

Vienotais ziņojuma formāts

1. Ar šo tiek izveidots vienotais ziņojuma formāts (*UMF*). *UMF* nosaka standartus konkrētiem satura elementiem attiecībā uz pārrobežu informācijas apmaiņu starp informācijas sistēmām, iestādēm vai organizācijām tieslietu un iekšlietu jomā.

2. *UMF* standartu, ja tas ir iespējams, izmanto IIS, *ETIAS*, *ESP*, *CIR* un *MID* izstrādē, kā arī – vajadzības gadījumā – jaunu informācijas apmaiņas modeļu un informācijas sistēmu izstrādē, ko tieslietu un iekšlietu jomā veic *eu-LISA* vai jebkura cita Savienības aģentūra.

3. Komisija pieņem īstenošanas aktu, lai noteiktu un izstrādātu šā panta 1. punktā minēto *UMF* standartu. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

39. pants

Centrālais ziņošanas un statistikas repozitorijs

1. Izveido centrālu ziņošanas un statistikas repozitoriju (*CRRS*), lai saskaņā ar attiecīgajiem tiesību instrumentiem, kas reglamentē IIS, VIS, *ETIAS* un *SIS*, atbalstītu minēto sistēmu mērķus un lai politikas, operatīvos un datu kvalitātes nolūkos nodrošinātu vairākas sistēmas aptverošus statistikas datus un analītiskus ziņojumus.

2. *eu-LISA* savos tehniskajos centros izveido, ievieš un mitina *CRRS*, kurā ietverti dati un statistika, kas minēti Regulas (ES) 2017/2226 63. pantā, Regulas (EK) Nr. 767/2008 17. pantā, Regulas (ES) 2018/1240 84. pantā, Regulas (ES) 2018/1861 60. pantā un Regulas (ES) 2018/1860 16. pantā, un kas ir loģiski nodalīti atbilstoši ES informācijas sistēmai. Iestādēm, kas minētas Regulas (ES) 2017/2226 63. pantā, Regulas (EK) Nr. 767/2008 17. pantā, Regulas (ES) 2018/1240 84. pantā un Regulas (ES) 2018/1861 60. pantā, piešķir piekļuvi *CRRS* tikai pārskatu un statistikas vajadzībām, izmantojot kontrolētu, drošu piekļuvi un īpašus lietotāju profilus.

3. *eu-LISA* padara datus anonīmus un reģistrē šādus anonimizētus datus *CRRS*. Process, kura gaitā datus padara anonīmus, ir automatizēts.

CRRS ietvertie dati nedod iespēju identificēt privātpersonas.

4. *CRRS* veido:

a) datu anonimizēšanai nepieciešamie rīki;

b) centrāla infrastruktūra, kas sastāv no datu repozitorija, kurā ir anonīmi dati;

c) droša komunikācijas infrastruktūra, kuras mērķis ir savienot *CRRS* ar IIS, VIS, *ETIAS* un *SIS*, kā arī ar kopējā *BMS*, *CIR* un *MID* centrālajām infrastruktūrām.

5. Komisija pieņem deleģētu aktu saskaņā ar 73. pantu, paredzot sīki izstrādātus noteikumus par *CRRS* darbību, tostarp īpašus aizsardzības pasākumus personas datu apstrādei atbilstīgi šā panta 2. un 3. punktam un drošības noteikumus, kas piemērojami repozitorijam.

([39]) Padomes Regula (EK) Nr. 168/2007 (2007. gada 15. februāris), ar ko izveido Eiropas Savienības Pamattiesību aģentūru (OV L 53, 22.2.2007., 1. lpp.).

VII NODAĻA

Datu aizsardzība

40. pants

Datu pārzinis

1. Saistībā ar datu apstrādi kopējā *BMS* dalībvalstu iestādes, kas attiecīgi ir pārziņi attiecībā uz IIS, VIS un *SIS*, ir pārziņi arī saskaņā ar Regulas (ES) 2016/679 4. panta 7. punktu vai Direktīvas (ES) 2016/680 3. panta 8. punktu attiecībā uz biometriskajām veidnēm, kuras iegūtas no šīs regulas 13. pantā minētajiem datiem, ko tās ievada pamatā esošajās sistēmās, un minētās iestādes ir atbildīgas par biometrisko veidņu apstrādi kopējā *BMS*.

2. Saistībā ar datu apstrādi *CIR* dalībvalstu iestādes, kas attiecīgi ir pārziņi attiecībā uz IIS, VIS un *ETIAS*, ir pārziņi arī saskaņā ar Regulas (ES) 2016/679 4. panta 7) punktu attiecībā uz šīs regulas 18. pantā minētajiem datiem, kurus tās ievada pamatā esošajās sistēmās, un minētās iestādes ir atbildīgas par minēto personas datu apstrādi *CIR*.

3. Attiecībā uz datu apstrādi *MID*:

a) Eiropas Robežu un krasta apsardzes aģentūra ir datu pārzinis Regulas (ES) 2018/1725 3. panta 8) punkta nozīmē attiecībā uz personas datu apstrādi, ko veic *ETIAS* centrālā vienība;

b) dalībvalstu iestādes, kas papildina vai groza identitātes apstiprinājuma datnē ietvertos datus, ir pārziņi saskaņā ar Regulas (ES) 2016/679 4. panta 7) punktu vai Direktīvas (ES) 2016/680 3. panta 8) punktu, un minētās iestādes ir atbildīgas par personas datu apstrādi *MID*;

4. Datu aizsardzības uzraudzības nolūkā, tostarp nolūkā pārbaudīt vaicājuma pieļaujamību un datu apstrādes likumību, datu pārziņiem ir piekļuve 10., 16., 24. un 36. pantā minētajiem reģistra ierakstiem pašuzraudzības vajadzībām, kā minēts 44. pantā.

41. pants

Datu apstrādātājs

Attiecībā uz personas datu apstrādi kopējā *BMS*, *CIR* un *MID* *eu-LISA* ir datu apstrādātājs Regulas (ES) 2018/1725 3. panta 12. punkta a) apakšpunkta nozīmē.

42. pants

Apstrādes drošība

1. *eu-LISA*, *ETIAS* centrālā vienība, Eiropols un dalībvalstu iestādes nodrošina saskaņā ar šo regulu veiktās personu datu apstrādes drošību. *eu-LISA*, *ETIAS* centrālā vienība, Eiropols un dalībvalstu iestādes sadarbojas ar drošību saistītajos uzdevumos.

2. Neskarot Regulas (ES) 2018/1725 33. pantu, *eu-LISA* veic vajadzīgos pasākumus, lai nodrošinātu sadarbspējas komponentu un ar tiem saistītās komunikācijas infrastruktūras drošību.

3. Jo īpaši *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 nepiederošām personām piekļuvi datu apstrādes aprīkojumam un iekārtām;

c) novērstu datu neatļautu nolasīšanu, kopēšanu, grozīšanu vai datu nesēju izņemšanu;

d) novērstu datu nesankcionētu ievadīšanu, kā arī liegtu reģistrēto personas datu nesankcionētu apskati, grozīšanu vai dzēšanu;

e) novērstu datu nesankcionētu apstrādi, kā arī datu nesankcionētu kopēšanu, grozīšanu vai dzēšanu;

f) liegtu iespēju nepilnvarotām personām, kas izmanto datu pārraides ierīces, lietot automatizētas datu apstrādes sistēmas;

g) nodrošinātu, ka personām, kas ir pilnvarotas piekļūt sadarbspējas komponentiem, ir piekļuve tikai tiem datiem, uz kuriem attiecas viņu piekļuves tiesības, izmantojot tikai individuālas lietotāju identitātes un konfidenciālus piekļuves režīmus;

h) nodrošinātu to, ka var pārbaudīt un noteikt, kurām struktūrām personas datus var pārraidīt, izmantojot datu pārraides ierīces;

i) nodrošinātu iespēju pārbaudīt un noteikt, kādi dati ir apstrādāti sadarbspējas komponentos, kad, kas un kādam mērķim tos ir apstrādājis;

j) nodrošinātu, jo īpaši ar pienācīgu šifrēšanas paņēmienu palīdzību, ka laikā, kad personu datus pārraida uz sadarbspējas komponentiem vai no tiem, vai datu nesēju transportēšanas laikā tos nevar nesankcionēti nolasīt, kopēt, grozīt vai dzēst;

k) nodrošinātu, ka traucējuma gadījumā ir iespējams atjaunot uzstādīto sistēmu normālu darbību;

l) nodrošinātu uzticamību, garantējot, ka jebkuras sadarbspējas komponentu darbības kļūmes tiek pienācīgi darītas zināmas;

m) uzraudzītu šajā punktā minēto drošības pasākumu efektivitāti un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību ar mērķi nodrošināt atbilstību šai regulai un novērtēt šos drošības pasākumus, ņemot vērā jaunos tehnoloģiskos sasniegumus.

4. Dalībvalstis, Eiropols un *ETIAS* centrālā vienība pieņem 3. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar personas datu apstrādi, ko veic iestādes, kurām ir tiesības piekļūt jebkuram sadarbspējas komponentam.

43. pants

Drošības incidenti

1. Jebkuru notikumu, kas ietekmē vai var ietekmēt sadarbspējas komponentu drošību un var kaitēt tajos glabātajiem datiem vai izraisīt to zudumu, uzskata par drošības incidentu, jo īpaši, ja ir notikusi nesankcionēta piekļuve datiem vai ir apdraudēta vai varētu būt tikusi apdraudēta datu pieejamība, integritāte un konfidencialitāte.

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

3. Neskarot Regulas (ES) 2016/679 33. pantā, Direktīvas (ES) 2016/680 30. pantā vai abos paredzēto paziņošanu par personas datu aizsardzības pārkāpumu, dalībvalstis nekavējoties paziņo Komisijai, *eu-LISA*, kompetentajām uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītājam par visiem drošības incidentiem.

Neskarot Regulas (ES) 2018/1725 34. un 35. pantu un Regulas (ES) 2016/794 34. pantu, *ETIAS* centrālā vienība un Eiropols nekavējoties paziņo Komisijai, *eu-LISA* un Eiropas Datu aizsardzības uzraudzītājam par visiem drošības incidentiem.

Ja noticis drošības incidents saistībā ar sadarbspējas komponentu centrālo infrastruktūru, *eu-LISA* par to nekavējoties paziņo Komisijai un Eiropas Datu aizsardzības uzraudzītājam.

4. Informāciju par drošības incidentu, kam ir vai var būt ietekme uz sadarbspējas komponentu darbību vai uz datu pieejamību, integritāti un konfidencialitāti, nekavējoties sniedz dalībvalstīm, *ETIAS* centrālajai vienībai, un Eiropolam, un par to ziņo atbilstīgi incidentu pārvaldības plānam, ko nodrošina *eu-LISA*.

5. Attiecīgās dalībvalstis, *ETIAS* centrālā vienība, Eiropols un *eu-LISA* drošības incidenta gadījumā sadarbojas. Komisija ar īstenošanas aktiem nosaka šīs sadarbības procedūras kārtību. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

44. pants

Pašuzraudzība

Dalībvalstis un attiecīgās Savienības aģentūras nodrošina, ka katra iestāde, kurai ir tiesības piekļūt sadarbspējas komponentiem, veic vajadzīgos pasākumus, lai uzraudzītu savu atbilstību šai regulai, un vajadzības gadījumā sadarbojas ar uzraudzības iestādi.

Šīs regulas 40. pantā minētie datu pārziņi veic vajadzīgos pasākumus, lai uzraudzītu saskaņā ar šo regulu veiktās datu apstrādes atbilstību, tostarp bieži pārbaudot 10., 16., 24. un 36. pantā minētos reģistra ierakstus, un vajadzības gadījumā sadarbojas ar uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju.

45. pants

Sankcijas

Dalībvalstis nodrošina, ka par jebkādu datu nepareizu izmantošanu, datu apstrādi vai datu apmaiņu, kas ir pretrunā šai regulai, piemēro sankcijas saskaņā ar valsts tiesību aktiem. Paredzētās sankcijas ir efektīvas, samērīgas un atturošas.

46. pants

Atbildība

1. Neskarot tiesības uz kompensāciju no pārziņa vai apstrādātāja un pārziņa vai apstrādātāja atbildību saskaņā ar Regulu (ES) 2016/679, Direktīvu (ES) 2016/680 un Regulu (ES) 2018/1725:

a) jebkurai personai vai dalībvalstij, kurai ir nodarīts materiāls vai nemateriāls kaitējums tādas nelikumīgas personas datu apstrādes darbības vai jebkuras citas ar šo regulu nesaderīgas tādas rīcības rezultātā, kuru ir veikusi dalībvalsts, ir tiesības saņemt kompensāciju no minētās dalībvalsts;

b) jebkurai personai vai dalībvalstij, kam nodarīts materiāls vai nemateriāls kaitējums ar šo regulu nesaderīgas rīcības rezultātā, kuru veicis Eiropols, Eiropas Robežu un krasta apsardzes aģentūra vai *eu-LISA*, ir tiesības saņemt kompensāciju no minētās aģentūras.

Attiecīgo dalībvalsti, Eiropolu, Eiropas Robežu un krasta apsardzes aģentūru vai *eu-LISA* pilnībā vai daļēji atbrīvo no pirmajā daļā noteiktās atbildības, ja tie pierāda, ka nav atbildīgi par notikumu, kas ir izraisījis minēto kaitējumu.

2. Ja sakarā ar to, ka kāda dalībvalsts nav ievērojusi šajā regulā noteiktus pienākumus, ir nodarīts kaitējums sadarbspējas komponentiem, minētā dalībvalsts ir atbildīga par šādu kaitējumu, izņemot gadījumu, kad un ciktāl *eu-LISA* vai cita dalībvalsts, kurai ir jāievēro šī regula, nav veikusi saprātīgus pasākumus, lai kaitējumu novērstu vai mazinātu tā sekas.

3. Pret dalībvalsti vērstas prasības attiecībā uz kompensāciju par kaitējumu, kas ir minēts 1. un 2. punktā, reglamentē atbildētājas dalībvalsts tiesību akti. Pret pārzini vai *eu-LISA* vērstām kompensācijas prasībām par kaitējumu, kas ir minēts 1. un 2. punktā, piemēro Līgumos paredzētos nosacījumus.

47. pants

Tiesības uz informāciju

1. Iestāde, kas vāc personas datus, kuri glabājami kopējā *BMS*, *CIR* vai *MID*, sniedz personām, kuru dati tiek vākti, informāciju, kas jāsniedz saskaņā ar Regulas (ES) 2016/679 13. un 14. pantu, Direktīvas (ES) 2016/680 12. un 13. pantu un Regulas (ES) 2018/1725 15. un 16. pantu. Minētā iestāde sniedz informāciju brīdī, kad šādus datus ievāc.

2. Informāciju dara pieejamu skaidrā un vienkāršā valodā tādas valodas versijā, kuru attiecīgā persona saprot vai par kuru var pamatoti sagaidīt, ka tā to saprot. Tas attiecas arī uz vecumam atbilstošu informācijas sniegšanu datu subjektiem, kuri ir nepilngadīgie.

3. Personas, kuru dati ir reģistrēti IIS, VIS vai *ETIAS*, saskaņā ar 1. punktu tiek informētas par personas datu apstrādi, ko veic šīs regulas vajadzībām, ja:

a) IIS saskaņā ar Regulas (ES) 2017/226 14. pantu ir izveidota vai atjaunināta personas datne;

b) VIS saskaņā ar Regulas (EK) Nr. 767/2008 8. pantu ir izveidota vai atjaunināta pieteikuma datne;

c) *ETIAS* saskaņā ar Regulas (ES) 2018/1240 19. pantu ir izveidota vai atjaunināta pieteikuma datne.

48. pants

Tiesības piekļūt MID glabātajiem personas datiem, tos labot un dzēst un ierobežot to apstrādi

1. Lai īstenotu Regulas (ES) 2016/679 15. līdz 18. pantā, Regulas (ES) 2018/1725 17. līdz 20. pantā un Direktīvas (ES) 2016/680 14., 15. un 16. pantā noteiktās tiesības, ikvienai personai ir tiesības vērsties jebkuras dalībvalsts kompetentajā iestādē, kas izskata pieprasījumu un atbild uz to.

2. Dalībvalsts, kura izskata šādu pieprasījumu, atbild bez nepamatotas kavēšanās un jebkurā gadījumā ne vēlāk kā 45 dienu laikā pēc pieprasījuma saņemšanas. Vajadzības gadījumā minēto laikposmu var pagarināt vēl par 15 dienām, ņemot vērā pieprasījumu sarežģītību un skaitu. Dalībvalsts, kura izskata šādu pieprasījumu, informē datu subjektu par jebkuru šādu pagarinājumu un kavēšanās iemesliem 45 dienu laikā pēc pieprasījuma saņemšanas. Dalībvalstis var nolemt, ka atbildes sniedz centrālie biroji.

3. Ja personas datu labošanas vai dzēšanas pieprasījumu iesniedz citai dalībvalstij, nevis par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai dalībvalstij, tās dalībvalsts iestādes, kurām pieprasījums iesniegts, septiņu dienu laikā sazinās ar tās dalībvalsts iestādēm, kas atbildīga par atšķirīgu identitāšu manuālu verifikāciju. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts bez nepamatotas kavēšanās un jebkurā gadījumā 30 dienu laikā pēc šādas sazināšanās pārbauda datu pareizību un datu apstrādes likumību. Vajadzības gadījumā minēto laikposmu var pagarināt vēl par 15 dienām, ņemot vērā pieprasījumu sarežģītību un skaitu. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts informē dalībvalsti, kura ar to sazinājusies, par jebkuru šādu pagarinājumu un par kavēšanās iemesliem. Dalībvalsts, kas ir sazinājusies ar tās dalībvalsts iestādi, kura atbildīga par atšķirīgu identitāšu manuālu verifikāciju, informē attiecīgo personu par turpmāko procedūru.

4. Ja personas datu labošanas vai dzēšanas pieprasījumu iesniedz dalībvalstij un ja par atšķirīgu identitāšu manuālu verifikāciju bija atbildīga *ETIAS* centrālā vienība, tās dalībvalsts iestādes, kurām pieprasījums iesniegts, septiņu dienu laikā sazinās ar *ETIAS* centrālo vienību un lūdz tai sniegt atzinumu. *ETIAS* centrālā vienība sniedz atzinumu bez nepamatotas kavēšanās un jebkurā gadījumā 30 dienu laikā pēc sazināšanās ar to. Vajadzības gadījumā minēto laikposmu var pagarināt vēl par 15 dienām, ņemot vērā pieprasījumu sarežģītību un skaitu. Dalībvalsts, kura sazinājās ar *ETIAS* centrālo vienību, informē attiecīgo personu par turpmāko procedūru.

5. Ja pēc pārbaudes tiek konstatēts, ka *MID* glabātie dati ir neprecīzi vai ir reģistrēti nelikumīgi, tad par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts vai, ja par atšķirīgu identitāšu manuālu verifikāciju nebija atbildīga neviena dalībvalsts vai ja par atšķirīgu identitāšu manuālu verifikāciju bija atbildīga *ETIAS* centrālā vienība, dalībvalsts, kurai iesniegts pieprasījums, bez nepamatotas kavēšanās labo vai dzēš minētos datus. Attiecīgo personu rakstiski informē, ka tās dati ir laboti vai dzēsti.

6. Ja dalībvalsts ievieš grozījumus *MID* glabātajos datos to saglabāšanas periodā, attiecīgā dalībvalsts veic 27. pantā un – vajadzības gadījumā – 29. pantā paredzēto apstrādi, lai noteiktu, vai grozītie dati ir jāsaista. Ja apstrāde neuzrāda nevienu atbilstību, attiecīgā dalībvalsts dzēš datus no identitātes apstiprinājuma datnes. Ja automatizētā apstrāde uzrāda vienu vai vairākas atbilstības, attiecīgā dalībvalsts izveido vai atjaunina attiecīgo saikni saskaņā ar attiecīgajiem šīs regulas noteikumiem.

7. Ja par atšķirīgo identitāšu manuālu verifikāciju atbildīgā dalībvalsts vai – vajadzības gadījumā – dalībvalsts, kurai iesniegts pieprasījums, nepiekrīt tam, ka *MID* glabātie dati ir neprecīzi vai ir reģistrēti nelikumīgi, minētā dalībvalsts pieņem administratīvu lēmumu, kurā attiecīgajai personai nekavējoties rakstiski paskaidrots, kāpēc valsts atsakās labot vai dzēst datus, kas attiecas uz šo personu.

8. Ar 7. punktā minēto lēmumu attiecīgajai personai arī sniedz informāciju, kurā izskaidrota iespēja pārsūdzēt lēmumu, kas pieņemts saistībā ar pieprasījumu piekļūt personas datiem, tos labot, dzēst vai ierobežot to apstrādi, un – vajadzības gadījumā – informāciju par to, kā celt prasību vai iesniegt sūdzību kompetentajās iestādēs vai tiesās, kā arī informāciju par jebkādu palīdzību, tostarp uzraudzības iestāžu palīdzību.

9. Visos pieprasījumos piekļūt personas datiem, tos labot vai dzēst vai ierobežot to apstrādi ietver informāciju, kura vajadzīga, lai identificētu attiecīgo personu. Minēto informāciju izmanto vienīgi tam, lai varētu īstenot šajā pantā minētās tiesības, un pēc tam to nekavējoties dzēš.

10. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts vai – vajadzības gadījumā – dalībvalsts, kurai iesniegts pieprasījums, rakstveidā glabā ierakstu, ka tika iesniegts pieprasījums piekļūt personas datiem, tos labot vai dzēst vai ierobežot to apstrādi, un to, kā tas tika izskatīts, un nekavējoties dara minēto ierakstu pieejamu uzraudzības iestādēm.

11. Šis pants neskar nekādus šajā pantā minēto tiesību ierobežojumus, kas paredzēti saskaņā ar Regulu (ES) 2016/679 un Direktīvu (ES) 2016/680.

49. pants

Tīmekļa portāls

1. Lai būtu vieglāk izmantot tiesības piekļūt personas datiem, tos labot vai dzēst vai ierobežot to apstrādi, izveido tīmekļa portālu.

2. Tīmekļa portālā ir informācija par 47. un 48. pantā minētajām tiesībām un procedūrām un lietotāja saskarne, kas personām, kuru datus apstrādā *MID* un kuras tika informētas par sarkanas saiknes esamību saskaņā ar 32. panta 4. punktu, sniedz iespēju saņemt par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes kontaktinformāciju.

3. Lai iegūtu par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes kontaktinformāciju, personai, kuru datus apstrādā *MID*, būtu jāievada 34. panta d) punktā minētā atsauce uz iestādi, kas atbild par atšķirīgu identitāšu manuālu verifikāciju. Tīmekļa portāls izmanto šo atsauci, lai izgūtu par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes kontaktinformāciju. Tīmekļa portālā ir iekļauta arī e-pasta ziņojuma veidne, kuras nolūks ir atvieglot portāla lietotāja un par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes saziņu. Šādā e-pasta ziņojumā ietver lauku 34. panta c) punktā minētajam vienotajam identifikācijas numuram, lai par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentā iestāde varētu identificēt attiecīgos datus.

4. Dalībvalstis nodrošina *eu-LISA* visu to iestāžu kontaktinformāciju, kuras ir kompetentas izskatīt jebkuru 47. un 48. pantā minēto pieprasījumu un atbildēt uz to, un regulāri pārbauda, vai minētā kontaktinformācija ir aktualizēta.

5. *eu-LISA* izstrādā tīmekļa portālu un nodrošina tā tehnisko pārvaldību.

6. Komisija pieņem deleģēto aktu saskaņā ar 73. pantu, paredzot sīki izstrādātus noteikumus par tīmekļa portāla darbību, tostarp lietotāja saskarni, valodām, kurās tīmekļa portāls ir pieejams un e-pasta ziņojuma veidni.

50. pants

Personas datu nodošana trešām valstīm, starptautiskām organizācijām un privātām struktūrām

Neskarot Regulas (ES) 2018/1240 65. pantu, Regulas (ES) 2016/794 25. un 26. pantu, Regulas (ES) 2017/2226 41. pantu, Regulas (EK) Nr. 767/2008 31. pantu un tādus vaicājumus Interpola datubāzēs, kas veikti, izmantojot *ESP* saskaņā ar šīs regulas 9. panta 5. punktu, un atbilst Regulas (ES) 2018/1725 V nodaļas noteikumiem un Regulas (ES) 2016/679 V nodaļas noteikumiem, personas datus, kuri tiek glabāti sadarbspējas komponentos vai kurus apstrādā vai kuriem piekļūst ar sadarbspējas komponentu palīdzību, nenosūta vai nedara pieejamus nevienai trešai valstij, starptautiskai organizācijai vai privātai struktūrai.

51. pants

Uzraudzība, ko veic uzraudzības iestādes

1. Katra dalībvalsts nodrošina, ka uzraudzības iestādes neatkarīgi uzrauga personas datu apstrādes, ko attiecīgā dalībvalsts veic atbilstīgi šai regulai, tostarp datu pārraidīšanas uz sadarbspējas komponentiem un no tiem, likumību.

2. Katra dalībvalsts nodrošina, ka tās normatīvo un administratīvo aktu noteikumi, kas ir pieņemti, ievērojot Direktīvu (ES) 2016/680, vajadzības gadījumā ir piemērojami arī attiecībā uz policijas iestāžu un izraudzīto iestāžu piekļuvi sadarbspējas komponentiem, tostarp attiecībā uz to personu tiesībām, kuru datiem šādā veidā tās piekļūst.

3. Uzraudzības iestādes nodrošina, ka vismaz reizi četros gados tiek veikta to personas datu apstrādes darbību revīzija, ko veikušas atbildīgās valsts iestādes šīs regulas nolūkos, saskaņā ar attiecīgiem starptautiskiem revīzijas standartiem.

Uzraudzības iestādes katru gadu publisko personas datu labošanas, dzēšanas vai apstrādes ierobežojumu pieprasījumu skaitu, informāciju par turpmāk veiktajām darbībām un pēc attiecīgo personu pieprasījuma veikto labojumu, dzēšanu un apstrādes ierobežojumu skaitu.

4. Dalībvalstis nodrošina uzraudzības iestādēm pietiekamus resursus un zinātību, lai tās veiktu ar šo regulu uzticētos uzdevumus.

5. Dalībvalstis sniedz jebkādu informāciju, ko ir pieprasījusi Regulas (ES) 2016/679 51. panta 1. punktā minētā uzraudzības iestāde, un jo īpaši tai sniedz informāciju par darbībām, kas ir veiktas saskaņā ar dalībvalstu pienākumiem, kas noteikti šajā regulā. Dalībvalstis nodrošina Regulas (ES) 2016/679 51. panta 1. punktā minētajām uzraudzības iestādēm piekļuvi saviem reģistra ierakstiem, kas minēti šīs regulas 10., 16., 24. un 36. pantā, saviem pamatojumiem, kas minēti šīs regulas 22. panta 2. punktā, un ļauj tām jebkurā laikā iekļūt visās savās sadarbspējas nolūkā izmantotajās telpās.

52. pants

Revīzijas, ko veic Eiropas Datu aizsardzības uzraudzītājs

Eiropas Datu aizsardzības uzraudzītājs nodrošina, ka vismaz reizi četros gados tiek veikta *eu-LISA*, *ETIAS* centrālās vienības un Eiropola šīs regulas nolūkos veikto personas datu apstrādes darbību revīzija saskaņā ar attiecīgiem starptautiskiem revīzijas standartiem. Ziņojumu par minēto revīziju nosūta Eiropas Parlamentam, Padomei, *eu-LISA*, Komisijai, dalībvalstīm un attiecīgajai Savienības aģentūrai. Pirms ziņojumu pieņemšanas *eu-LISA*, *ETIAS* centrālajai vienībai un Eiropolam dod iespēju izteikt savus apsvērumus.

eu-LISA, *ETIAS* centrālā vienība un Eiropols sniedz Eiropas Datu aizsardzības uzraudzītājam tā pieprasīto informāciju, piešķir Eiropas Datu aizsardzības uzraudzītājam piekļuvi visiem dokumentiem, ko tas pieprasa, un saviem reģistra ierakstiem, kas ir minēti 10., 16., 24. un 36. pantā, un ļauj Eiropas Datu aizsardzības uzraudzītājam jebkurā laikā iekļūt visās to telpās.

53. pants

Uzraudzības iestāžu un Eiropas Datu aizsardzības uzraudzītāja sadarbība

1. Uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs, katrs rīkojoties savas attiecīgās kompetences robežās, aktīvi sadarbojas, ievērojot savus attiecīgos pienākumus, un nodrošina koordinētu sadarbspējas komponentu izmantošanas un šīs regulas noteikumu piemērošanas uzraudzību, jo īpaši tad, ja Eiropas Datu aizsardzības uzraudzītājs vai uzraudzības iestāde konstatē nozīmīgas neatbilstības Eiropas Savienības dalībvalstu praksē vai atklāj, iespējams, nelikumīgu nosūtīšanu, kas veikta, izmantojot sadarbspējas komponentu sakaru kanālus.

2. Gadījumos, kas minēti šā panta 1. punktā, nodrošina koordinētu uzraudzību saskaņā ar Regulas (ES) 2018/1725 62. pantu.

3. Eiropas Datu aizsardzības kolēģija Eiropas Parlamentam, Padomei, Komisijai, Eiropolam, Eiropas Robežu un krasta apsardzes aģentūrai un *eu-LISA* līdz 2021. gada 12. jūnijam un reizi divos gados pēc tam nosūta kopīgu ziņojumu par savu darbību atbilstīgi šim pantam. Minētajā ziņojumā iekļauj nodaļu par katru dalībvalsti, ko sagatavo attiecīgās dalībvalsts uzraudzības iestāde.

VIII NODAĻA

Pienākumi

54. pants

eu-LISA pienākumi plānošanas un izstrādes posmā

1. *eu-LISA* nodrošina to, ka sadarbspējas komponentu centrālās infrastruktūras ekspluatē saskaņā ar šo regulu.

2. *eu-LISA* savos tehniskajos centros mitina sadarbspējas komponentus un nodrošina šajā regulā noteiktās funkcijas saskaņā ar 55. panta 1. punktā minētajiem drošības, pieejamības, kvalitātes un veiktspējas nosacījumiem.

3. *eu-LISA* ir atbildīga par sadarbspējas komponentu izstrādi un par jebkādiem pielāgojumiem, kas vajadzīgi, lai izveidotu sadarbspēju starp IIS, VIS, *ETIAS*, *SIS*, *Eurodac* un *ECRIS-TCN* centrālajām sistēmām, kā arī *ESP*, kopējo *BMS*, *CIR*, *MID* un *CRRS*.

Neskarot 66. pantu, *eu-LISA* nav piekļuves nekādiem personas datiem, kurus apstrādā, izmantojot *ESP*, kopējo *BMS*, *CIR* vai *MID*.

eu-LISA nosaka plānojumu sadarbspējas komponentu, tostarp to komunikācijas infrastruktūras un tehnisko specifikāciju, fiziskajai arhitektūrai, kā arī to attīstību attiecībā uz centrālo infrastruktūru un drošu komunikācijas infrastruktūru; minēto plānojumu pieņem valde, ņemot vērā Komisijas labvēlīgu atzinumu. *eu-LISA* arī ievieš visus nepieciešamos pielāgojumus IIS, VIS, *ETIAS* vai *SIS*, kuri izriet no sadarbspējas izveides un ir paredzēti šajā regulā.

eu-LISA izstrādā un ievieš sadarbspējas komponentus cik vien drīz iespējams pēc šīs regulas stāšanās spēkā un pēc tam, kad Komisija ir pieņēmusi 8. panta 2. punktā, 9. panta 7. punktā, 28. panta 5. un 7. punktā, 37. panta 4. punktā, 38. panta 3. punktā, 39. panta 5. punktā, 43. panta 5. punktā un 78. panta 10. punktā paredzētos pasākumus.

Izstrāde sastāv no tehnisko specifikāciju izstrādes un ieviešanas, testēšanas un projekta vispārējās vadības un koordinācijas.

4. Plānošanas un izstrādes posmā izveido Programmu vadības valdi, kurā ietilpst ne vairāk kā 10 locekļi. Tās sastāvā ir septiņi locekļi, kurus ieceļ *eu-LISA* valde no savu locekļu vai aizstājēju vidus, 75. pantā minētās padomdevēju grupas sadarbspējas jautājumos priekšsēdētājs, viens loceklis, kas pārstāv *eu-LISA* un ko iecēlis tās izpilddirektors, un viens Komisijas iecelts loceklis. *eu-LISA* valdes ieceltos locekļus ievēlē tikai no tām dalībvalstīm, kurām saskaņā ar Savienības tiesību aktiem ir pilnībā saistoši tiesību instrumenti, ar ko reglamentē visu ES informācijas sistēmu izstrādi, izveidi, darbību un izmantošanu, un kuras piedalīsies sadarbspējas komponentos.

5. Programmu vadības valde tiekas regulāri un vismaz trīs reizes ceturksnī. Tā nodrošina sadarbspējas komponentu plānošanas un izstrādes posma pienācīgu pārvaldību.

Programmu vadības valde katru mēnesi *eu-LISA* valdei iesniedz rakstiskus ziņojumus par projekta progresu. Programmu vadības valdei nav lēmumu pieņemšanas pilnvaru, nedz arī pilnvaru pārstāvēt *eu-LISA* valdes locekļus.

6. *eu-LISA* valde nosaka Programmu vadības valdes reglamentu, kurā jo īpaši iekļauj noteikumus par:

a) priekšsēdētāju;

b) sanāksmju vietām;

c) sanāksmju sagatavošanu;

d) ekspertu pielaidi sanāksmēm;

e) komunikācijas plāniem, kas nodrošina,ka klāt neesošie valdes locekļi tiek pilnībā informēti.

Priekšsēdētāja vietu ieņem dalībvalsts, kurai saskaņā ar Savienības tiesību aktiem ir pilnībā saistoši tiesību instrumenti, ar ko reglamentē visu ES informācijas sistēmu izstrādi, izveidi, darbību un izmantošanu un kas piedalīsies sadarbspējas komponentos.

Visus ceļošanas un uzturēšanās izdevumus, kas rodas Programmu vadības valdes locekļiem, sedz *eu-LISA*, un *eu-LISA* reglamenta 10. pantu piemēro mutatis mutandis. *eu-LISA* Programmu vadības valdei nodrošina sekretariātu.

Šīs regulas 75. pantā minētā padomdevēju grupa sadarbspējas jautājumos regulāri tiekas līdz sadarbspējas komponentu darbības uzsākšanai. Pēc katras sanāksmes tā ziņo Programmu vadības valdei. Tā nodrošina tehnisko zinātību, lai sniegtu atbalstu Programmu vadības valdes uzdevumu veikšanā, un seko līdzi dalībvalstu gatavības situācijai.

55. pants

eu-LISA pienākumi pēc darbības uzsākšanas

1. Pēc katra sadarbspējas komponenta darbības uzsākšanas *eu-LISA* ir atbildīga par sadarbspējas komponentu centrālās infrastruktūras tehnisko pārvaldību, tostarp par to uzturēšanu un tehnoloģisko attīstību. Sadarbībā ar dalībvalstīm tā nodrošina, ka tiek izmantotas labākās pieejamās tehnoloģijas, pamatojoties uz izmaksu lietderīguma analīzi. *eu-LISA* ir atbildīga arī par 6., 12., 17., 25. un 39. pantā minētās komunikāciju infrastruktūras tehnisko pārvaldību.

Sadarbspējas komponentu tehniskā pārvaldība ir visi tie uzdevumi un tehniskie risinājumi, kuri vajadzīgi, lai 24 stundas diennaktī 7 dienas nedēļā nodrošinātu sadarbspējas komponentu darbību un nodrošinātu nepārtrauktus pakalpojumus dalībvalstīm un Savienības aģentūrām saskaņā ar šo regulu. Tā ietver uzturēšanas darbu un tehnisko izstrādi, kas vajadzīga, lai nodrošinātu, ka komponentu darbības tehniskā kvalitāte ir apmierinošā līmenī, jo īpaši attiecībā uz reakcijas laiku, kurš vajadzīgs, lai sazinātos ar centrālajām infrastruktūrām saskaņā ar tehniskajām specifikācijām.

Visus sadarbspējas komponentus izstrādā un pārvalda tā, lai nodrošinātu ātru, raitu, efektīvu un kontrolētu piekļuvi, komponentu un *MID*, kopējā *BMS* un *CIR* glabāto datu pilnīgu un nepārtrauktu pieejamību un reakcijas laiku saskaņā ar dalībvalstu iestāžu un Savienības aģentūru funkcionālajām vajadzībām.

2. Neskarot 17. pantu Eiropas Savienības Civildienesta noteikumos, *eu-LISA* piemēro pienācīgus noteikumus par dienesta noslēpumu vai citas līdzvērtīgas konfidencialitātes prasības visiem saviem darbiniekiem, kuriem jāstrādā ar sadarbspējas komponentos glabātiem datiem. Šis pienākums ir spēkā arī tad, kad šie darbinieki vairs nav attiecīgajā amatā vai darbā, vai pēc tam, kad ir izbeigta to darbība.

Neskarot 66. pantu, *eu-LISA* nav piekļuves nekādiem personas datiem, kurus apstrādā, izmantojot *ESP*, kopējo *BMS*, *CIR* vai *MID*.

3. *eu-LISA* izstrādā un uztur mehānismu un procedūras kopējā *BMS* un *CIR* glabāto datu kvalitātes pārbaudēm saskaņā ar 37. pantu.

4. *eu-LISA* arī veic uzdevumus, kas saistīti ar apmācības sniegšanu par sadarbspējas komponentu tehnisko izmantošanu.

56. pants

Dalībvalstu pienākumi

1. Katra dalībvalsts ir atbildīga par:

a) savienošanu ar *ESP* un *CIR* komunikācijas infrastruktūru;

b) esošo valsts sistēmu un infrastruktūru integrāciju ar *ESP*, *CIR* un *MID*;

c) savas esošās valsts infrastruktūras organizāciju, pārvaldību, darbību un uzturēšanu un tās savienošanu ar sadarbspējas komponentiem;

d) kompetento valsts iestāžu darbinieku, kuriem pienācīgā kārtā izsniegta atļauja, piekļuves *ESP*, *CIR* un *MID* pārvaldību un organizēšanu saskaņā ar šo regulu un minēto darbinieku un viņu profilu saraksta izveidi un regulāru atjaunināšanu;

e) 20. panta 5. un 6. punktā minēto leģislatīvo pasākumu pieņemšanu, lai identifikācijas nolūkos nodrošinātu piekļuvi *CIR*;

f) atšķirīgu identitāšu manuālu verifikāciju, kas minēta 29. pantā;

g) atbilstību saskaņā ar Savienības tiesību aktiem noteiktajām datu kvalitātes prasībām;

h) atbilstību katras ES informācijas sistēmas noteikumiem par personas datu drošību un integritāti;

i) visu to trūkumu novēršanu, kuri konstatēti Komisijas izvērtēšanas ziņojumā attiecībā uz datu kvalitāti, kurš minēts 37. panta 5. punktā.

2. Katra dalībvalsts savieno savas izraudzītās iestādes ar *CIR*.

57. pants

ETIAS centrālās vienības pienākumi

ETIAS centrālā vienība ir atbildīga par to, lai:

a) veiktu atšķirīgu identitāšu manuālu verifikāciju saskaņā ar 29. pantu;

b) veiktu 69. pantā minēto vairāku identitāšu konstatēšanu starp datiem, kas glabāti IIS, VIS, *Eurodac* un *SIS*.

IX NODAĻA

Grozījumi citos Savienības instrumentos

58. pants

Grozījumi Regulā (EK) Nr. 767/2008

Regulu (EK) Nr. 767/2008 groza šādi:

1) regulas 1. pantam pievieno šādu daļu:

"Glabājot kopējā identitātes repozitorijā (*CIR*), kas izveidots ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/817 (*) 17. panta 1. punktu, identitātes datus, ceļošanas dokumentu datus un biometriskos datus, VIS ļauj atvieglot VIS reģistrēto personu pareizu identifikāciju un palīdz to veikt atbilstīgi minētās regulas 20. panta nosacījumiem un mērķiem.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).";

2) regulas 4. pantam pievieno šādus punktus:

"12) "VIS dati" ir visi dati, kas tiek glabāti VIS centrālajā sistēmā un *CIR* saskaņā ar 9. līdz 14. pantu;

13) "identitātes dati" ir dati, kas minēti 9. panta 4. punkta a) un aa) apakšpunktā;

14) "pirkstu nospiedumu dati" ir dati, kas attiecas uz labās rokas rādītājpirksta, vidējā pirksta, zeltneša, mazā pirkstiņa un īkšķa, ja tādi ir, un kreisās rokas piecu pirkstu nospiedumiem;";

3) regulas 5. pantā iekļauj šādu punktu:

"1.a *CIR* ietver datus, kas minēti 9. panta 4. punkta a) līdz c) apakšpunktā un 5. un 6. punktā. Atlikušos VIS datus glabā VIS centrālajā sistēmā.";

4) regulas 6. panta 2. punktu aizstāj ar šādu:

"2. Piekļuve VIS, lai datus aplūkotu, ir atļauta vienīgi pienācīgi pilnvarotiem tādu valsts iestāžu darbiniekiem katrā dalībvalstī, kas ir kompetentas 15. līdz 22. pantā minētajām vajadzībām, un to katras dalībvalsts iestāžu pienācīgi pilnvarotiem darbiniekiem un to Savienības aģentūru pienācīgi pilnvarotiem darbiniekiem, kuras ir kompetentas Regulas (ES) 2019/817 20. un 21. pantā minētajām vajadzībām. Šādu piekļuvi ierobežo atbilstīgi apjomam, kādā dati ir vajadzīgi, lai veiktu pienākumus minētajām vajadzībām, kā arī samērīgi izvirzītajiem mērķiem.";

5) regulas 9. panta 4. punkta a) līdz c) apakšpunktu aizstāj ar šādiem:

"a) uzvārds; vārds vai vārdi; dzimšanas datums; dzimums;

aa) uzvārds dzimšanas brīdī (bijušais(-ie) uzvārds(-i)); dzimšanas vieta un valsts; pašreizējā valstspiederība un valstspiederība dzimšanas brīdī;

b) ceļošanas dokumenta vai dokumentu veids un numurs un ceļošanas dokumenta vai dokumentu izdevējas valsts trīs burtu kods;

c) ceļošanas dokumenta vai dokumentu derīguma beigu termiņš;

ca) iestāde, kas izdevusi ceļošanas dokumentu, un tā izdošanas datums;".

59. pants

Grozījumi Regulā (ES) 2016/399

Regulas (ES) 2016/399 8. pantā iekļauj šādu punktu:

"4.a Ja, personai iebraucot vai izbraucot, attiecīgo datubāzu aplūkošana, tostarp vairāku identitāšu detektora aplūkošana ar Eiropas meklēšanas portālu, – kas izveidoti attiecīgi ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/817 (*) 25. panta 1. punktu un 6. panta 1. punktu, – rada dzeltenu saikni vai ļauj konstatēt sarkanu saikni, robežsargs aplūko kopējo identitātes repozitoriju, kas izveidots ar minētās regulas 17. panta 1. punktu vai *SIS*, vai abus, lai novērtētu atšķirības saistītajos identitātes datos un ceļošanas dokumenta datos. Robežsargs veic jebkādu papildu pārbaudi, kas vajadzīga, lai pieņemtu lēmumu par saiknes statusu un krāsu.

Saskaņā ar Regulas (ES) 2019/817 69. panta 1. punktu šo punktu piemēro tikai pēc vairāku identitāšu detektora darbības uzsākšanas atbilstīgi minētās regulas 72. panta 4. punktam."

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.)."

60. pants

Grozījumi Regulā (ES) 2017/2226

Regulu (ES) 2017/2226 groza šādi:

1) regulas 1. pantam pievieno šādu punktu:

"3. Glabājot identitātes datus, ceļošanas dokumentu datus un biometriskos datus kopējā identitātes repozitorijā (*CIR*), kas izveidots ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/817 (*) 17. panta 1. punktu, IIS ļauj atvieglot IIS reģistrēto personu pareizu identifikāciju un palīdz to veikt atbilstīgi minētās regulas 20. panta nosacījumiem un mērķiem.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).";

2) regulas 3. panta 1. punktu groza šādi:

a) punkta 22) apakšpunktu aizstāj ar šādu:

"22) "IIS dati" ir visi dati, kas tiek glabāti IIS centrālajā sistēmā un *CIR* saskaņā ar 15. līdz 20. pantu;";

b) iekļauj šādu apakšpunktu:

"22.a) "identitātes dati" ir dati, kas minēti 16. panta 1. punkta a) apakšpunktā, kā arī attiecīgie dati, kas minēti 17. panta 1. punktā un 18. panta 1. punktā;";

c) pievieno šādus apakšpunktus:

"32) "*ESP*" ir Eiropas meklēšanas portāls, kas izveidots ar Regulas (ES) 2019/817 6. panta 1. punktu;

33) "*CIR*" ir kopējais identitātes repozitorijs, kas izveidots ar Regulas (ES) 2019/817 17.panta 1. punktu.";

3) regulas 6. panta 1. punktam pievieno šādu apakšpunktu:

"j) nodrošināt personu pareizu identifikāciju.";

4) regulas 7. pantu groza šādi:

a) panta 1. punktu groza šādi:

i) iekļauj šādu apakšpunktu:

"aa) kopējais identitātes repozitorijs (*CIR*), kā minēts Regulas (ES) 2019/817 17. panta 2. punkta a) apakšpunktā";

ii) punkta f) apakšpunktu aizstāj ar šādu:

"f) droša komunikāciju infrastruktūra starp IIS centrālo sistēmu un *ESP* un *CIR* centrālajām infrastruktūrām.";

b) iekļauj šādu punktu:

"1.a *CIR* ietver datus, kas minēti 16. panta 1. punkta a) līdz d) apakšpunktā, 17. panta 1. punkta a), b) un c) apakšpunktā un 18. panta 1. un 2. punktā. Atlikušos IIS datus glabā IIS centrālajā sistēmā.";

5) regulas 9. pantam pievieno šādu punktu:

"4. Piekļuvi IIS datiem, kas tiek glabāti *CIR*, paredz vienīgi to katras dalībvalsts iestāžu pienācīgi pilnvarotiem darbiniekiem un to Savienības aģentūru pienācīgi pilnvarotiem darbiniekiem, kuras ir kompetentas Regulas (ES) 2019/817 20. un 21. pantā noteiktajiem nolūkiem. Šāda piekļuve attiecas tikai uz datiem, kas vajadzīgi viņu uzdevumu pildīšanai minētajos nolūkos, un ir samērīga ar izvirzītajiem mērķiem.";

6) regulas 21. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Ja tehniski nav iespējams ievadīt datus IIS centrālajā sistēmā vai *CIR* vai ja IIS centrālā sistēma vai *CIR* nedarbojas, 16.–20. pantā minētos datus īslaicīgi uzglabā valsts vienotajā saskarnē. Ja tas nav iespējams, šos datus īslaicīgi glabā uz vietas elektroniskā formātā. Abos gadījumos datus ievada IIS centrālajā sistēmā vai *CIR*, tiklīdz tas tehniski ir iespējams vai ir novērsti sistēmas darbības traucējumi. Dalībvalstis veic atbilstošos pasākumus un izvērš nepieciešamo infrastruktūru, iekārtas un resursus, lai nodrošinātu, ka šādu vietējo īslaicīgo glabāšanu var veikt jebkurā laikā un attiecībā uz jebkuru šo valstu robežšķērsošanas vietu.";

b) panta 2. punkta pirmo daļu aizstāj ar šādu:

"2. Neskarot pienākumu veikt robežpārbaudes saskaņā ar Regulu (ES) 2016/399, izņēmuma gadījumā, kad tehniski nav iespējams ievadīt datus ne IIS centrālajā sistēmā, ne *CIR*, ne valsts vienotajā saskarnē un tehniski nav iespējams īslaicīgi saglabāt datus elektroniskā formātā uz vietas, robežu iestāde manuāli saglabā šīs regulas 16.–20. pantā minētos datus, izņemot biometriskos datus, un trešās valsts valstspiederīgā ceļošanas dokumentā iespiež spiedogu par ieceļošanu vai izceļošanu. Minētos datus ievada IIS centrālajā sistēmā un *CIR*, tiklīdz tas ir tehniski iespējams.";

7) regulas 23. pantu groza šādi:

a) iekļauj šādu punktu:

"2.a Šā panta 1. punktā noteikto verifikāciju veikšanas nolūkā robežu iestāde veic vaicājumu *ESP*, lai salīdzinātu datus par trešās valsts valstspiederīgo ar attiecīgajiem datiem, kas atrodami IIS un VIS.";

b) panta 4. punkta pirmo daļu aizstāj ar šādu:

"4. Ja, meklējot pēc šā panta 2. punktā paredzētajiem burtciparu datiem, noskaidrojas, ka trešās valsts valstspiederīgā dati nav reģistrēti IIS, ja trešās valsts valstspiederīgā pārbaude, ievērojot šā panta 2. punktu, nav izdevusies vai ja pastāv šaubas par trešās valsts valstspiederīgā identitāti, robežu iestādēm ir piekļuve datiem identifikācijas veikšanai saskaņā ar šīs regulas 27. pantu, lai izveidotu vai atjauninātu personas datni saskaņā ar 14. pantu.";

8) regulas 32. pantā iekļauj šādu punktu:

"1.a Gadījumos, kad izraudzītās iestādes veica vaicājumu *CIR* saskaņā ar Regulas (ES) 2019/817 22. pantu, tās var piekļūt IIS datu aplūkošanai, ja ir izpildīti šajā pantā paredzētie nosacījumi un ja saņemtajā atbildē, kas minēta Regulas (ES) 2019/817 22. panta 2. punktā, ir norādīts, ka dati tiek glabāti IIS.";

9) regulas 33. pantā iekļauj šādu punktu:

"1.a Gadījumos, kad Eiropols ir veicis vaicājumu *CIR* saskaņā ar Regulas (ES) 2019/817 22. pantu, tas var piekļūt IIS datu aplūkošanai, ja ir izpildīti šajā pantā paredzētie nosacījumi un ja saņemtajā atbildē, kas minēta Regulas (ES) 2019/817 22. panta 2. punktā, ir norādīts, ka dati tiek glabāti IIS.";

10) regulas 34. pantu groza šādi:

a) panta 1. un 2. punktā vārdus "IIS centrālajā sistēmā" aizstāj ar vārdiem "*CIR* un IIS centrālajā sistēmā";

b) panta 5. punktā vārdus "no IIS centrālās sistēmas" aizstāj ar vārdiem "no IIS centrālās sistēmas un no *CIR*";

11) regulas 35. panta 7. punktu aizstāj ar šādu:

"7. IIS centrālā sistēma un *CIR* nekavējoties informē visas dalībvalstis par IIS vai *CIR* datu dzēšanu un vajadzības gadījumā izņem tos no 12. panta 3. punktā minētā identificēto personu saraksta.";

12) regulas 36. pantā vārdus "IIS centrālo sistēmu" aizstāj ar vārdiem "IIS centrālo sistēmu un *CIR*";

13) regulas 37. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. *eu-LISA* ir atbildīga par IIS centrālās sistēmas un *CIR*, valstu vienoto saskarņu, komunikācijas infrastruktūras izstrādi un drošā sakaru kanāla izstrādi starp IIS centrālo sistēmu un VIS centrālo sistēmu. *eu-LISA* ir arī atbildīga par 13. pantā minētā tīmekļa pakalpojuma izstrādi saskaņā ar sīki izstrādātajiem noteikumiem, kuri minēti 13. panta 7. punktā, un specifikācijām un nosacījumiem, kuri pieņemti, ievērojot 36. panta pirmās daļas h) un j) apakšpunktu, un par 63. panta 2. punktā minētā datu repozitorija izstrādi.";

b) panta 3. punkta pirmo daļu aizstāj ar šādu:

"3. *eu-LISA* ir atbildīga par IIS centrālās sistēmas un *CIR*, valstu vienoto saskarņu un drošā sakaru kanāla starp IIS centrālo sistēmu un VIS centrālo sistēmu darbības pārvaldību. Tā sadarbībā ar dalībvalstīm nodrošina, lai IIS centrālās sistēmas un *CIR*, valstu vienoto saskarņu, komunikācijas infrastruktūras, drošo sakaru kanāla starp IIS centrālo sistēmu, un VIS centrālo sistēmu, 13. pantā minētā tīmekļa pakalpojuma un 63. panta 2. punktā minētā datu repozitorija vajadzībām vienmēr tiktu izmantota labākā pieejamā tehnoloģija, pamatojoties uz izmaksu un ieguvumu analīzi. *eu-LISA* ir atbildīga arī par komunikācijas infrastruktūras starp IIS centrālo sistēmu un valstu vienotajām saskarnēm darbības pārvaldību, kā arī par 13. pantā minēto tīmekļa pakalpojumu un 63. panta 2. punktā minēto datu repozitoriju.";

14) regulas 46. panta 1. punktam pievieno šādu apakšpunktu:

"f) atsauci uz Eiropas meklēšanas portāla izmantošanu, lai veiktu vaicājumu IIS, kā minēts Regulas (ES) 2019/817 7. panta 2. punktā.";

15) regulas 63. pantu groza šādi:

a) panta 2. punktu aizstāj ar šādu:

"2. Šā panta 1. punkta nolūkā *eu-LISA* glabā minētajā punktā minētos datus centrālajā ziņošanas un statistikas repozitorijā, kas minēts Regulas (ES) 2019/817 39. pantā.";

b) panta 4. punktam pievieno šādu daļu:

"Katras dienas statistikas datus glabā centrālajā ziņošanas un statistikas repozitorijā."

61. pants

Grozījumi Regulā (ES) 2018/1240

Regulu (ES) 2018/1240 groza šādi:

1) regulas 1. pantam pievieno šādu punktu:

"3. Glabājot identitātes datus un ceļošanas dokumenta datus kopējā identitātes repozitorijā (*CIR*), kas izveidots ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/817 (*) 17. panta 1. punktu, *ETIAS* ļauj atvieglot *ETIAS* reģistrēto personu pareizu identifikāciju un palīdz to veikt atbilstīgi minētās regulas 20. panta nosacījumiem un mērķiem.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).";

2) regulas 3. panta 1. punktam pievieno šādus apakšpunktus:

"23) "*CIR*" ir kopējais identitātes repozitorijs, kas izveidots ar Regulas (ES) 2019/817 17. panta 1. punktu;

24) "*ESP*" ir Eiropas meklēšanas portāls, kas izveidots ar Regulas (ES) 2019/817 6. panta 1. punktu;

25) "*ETIAS* centrālā sistēma" ir 6. panta 2. punkta a) apakšpunktā minētā centrālā sistēma kopā ar *CIR*, ciktāl *CIR* ir ietverti 6. panta 2.a punktā minētie dati;

26) "identitātes dati" ir dati, kas minēti 17. panta 2. punkta a), b) un c) apakšpunktā;

27) "ceļošanas dokumenta dati" ir dati, kas minēti 17. panta 2. punkta d) un e) apakšpunktā, un ceļošanas dokumenta izdevējas valsts trīs burtu kods, kā minēts 19. panta 3. punkta c) apakšpunktā;";

3) regulas 4. pantam pievieno šādu punktu:

"g) sekmē personu pareizu identifikāciju;";

4) regulas 6. pantu groza šādi:

a) panta 2. punktu groza šādi:

i) punkta a) apakšpunktu aizstāj ar šādu:

"a) centrālā sistēma, tostarp 34. pantā minētais *ETIAS* kontrolsaraksts;";

ii) iekļauj šādu apakšpunktu:

"aa) *CIR*;";

iii) punkta d) apakšpunktu aizstāj ar šādu:

"d) droša komunikāciju infrastruktūra starp centrālo sistēmu un *ESP* un *CIR* centrālajām infrastruktūrām;";

b) iekļauj šādu punktu:

"2.a *CIR* ir ietverti identitātes dati un ceļošanas dokumenta dati. Pārējos datus glabā centrālajā sistēmā.";

5) regulas 13. pantu groza šādi:

a) iekļauj šādu punktu:

"4.a Piekļuvi *ETIAS* identitātes datiem un ceļošanas dokumenta datiem, kas tiek glabāti *CIR*, arī paredz vienīgi to katras dalībvalsts iestāžu pienācīgi pilnvarotiem darbiniekiem un to Savienības aģentūru pienācīgi pilnvarotiem darbiniekiem, kuras ir kompetentas Regulas (ES) 2019/817 20. un 21. pantā noteiktajiem nolūkiem. Šāda piekļuve attiecas tikai uz datiem, kas vajadzīgi viņu uzdevumu pildīšanai minētajos nolūkos, un ir samērīga ar izvirzītajiem mērķiem.";

b) panta 5. punktu aizstāj ar šādu:

"5. Katra dalībvalsts izraugās kompetentās valsts iestādes, kas minētas šā panta 1., 2., 4. un 4.a punktā, un minēto iestāžu sarakstu nekavējoties paziņo *eu-LISA* saskaņā ar 87. panta 2. punktu. Minētajā sarakstā norāda, kādā nolūkā katras iestādes pienācīgi pilnvarotiem darbiniekiem ir piekļuve *ETIAS* informācijas sistēmā ietvertajiem datiem saskaņā ar šā panta 1., 2., 4. un 4.a punktu.";

6) regulas 17. panta 2. punktu groza šādi:

a) punkta a) apakšpunktu aizstāj ar šādu:

"a) uzvārdu, vārdu(-us), uzvārdu piedzimstot; dzimšanas datumu, dzimšanas vietu, dzimumu, pašreizējo valstspiederību;";

b) iekļauj šādu apakšpunktu:

"aa) dzimšanas valsti, pieteikuma iesniedzēja vecāku vārdu(-us);";

7) regulas 19. panta 4. punktā vārdus "17. panta 2. punkta a) apakšpunktā" aizstāj ar vārdiem "17. panta 2. punkta a) un aa) apakšpunktā";

8) regulas 20. pantu groza šādi:

a) panta 2. punkta pirmo daļu aizstāj ar šādu:

"2. *ETIAS* centrālā sistēma veic vaicājumu, izmantojot *ESP*, lai salīdzinātu 17. panta 2. punkta a), aa), b), c), d), f), g), j), k) un m) apakšpunktā un 17. panta 8. punktā minētos attiecīgos datus ar datiem ierakstā, datnē vai brīdinājumā, kas ir reģistrēts pieteikuma datnē, kura tiek glabāta *ETIAS* centrālajā sistēmā, *SIS*, IIS, VIS, *Eurodac*, Eiropola datos un Interpola *SLTD* un *TDAWN* datubāzēs.";

b) panta 4. punktā vārdus "17. panta 2. punkta a), b), c), d), f), g), j), k) un m) apakšpunktā" aizstāj ar vārdiem "17. panta 2. punkta a), aa), b), c), d), f), g), j), k) un m) apakšpunktā";

c) panta 5. punktā vārdus "17. panta 2. punkta a), c), f), h) un i) apakšpunktā" aizstāj ar vārdiem "17. panta 2. punkta a), aa), c), f), h) un i) apakšpunktā";

9) regulas 23. panta 1. punktu aizstāj ar šādu:

"1. *ETIAS* centrālā sistēma veic vaicājumu, izmantojot *ESP*, nolūkā salīdzināt 17. panta 2. punkta a), aa), b) un d) apakšpunktā minētos attiecīgos datus ar datiem *SIS*, lai noteiktu, vai uz pieteikuma iesniedzēju attiecas kāds no šiem brīdinājumiem:

a) brīdinājums par pazudušām personām;

b) brīdinājums attiecībā uz personām, ko cenšas atrast, lai tās varētu palīdzēt tiesas procesā;

c) brīdinājums par personām diskrētu pārbaužu vai īpašu pārbaužu vajadzībām.";

10) regulas 52. pantā iekļauj šādu punktu:

"1.a Gadījumos, kad izraudzītās iestādes ir veikušas vaicājumu *CIR* saskaņā ar Regulas (ES) 2019/817 22. pantu, minētās iestādes datu aplūkošanas nolūkā var piekļūt pieteikuma datnēm, ko *ETIAS* centrālajā sistēmā glabā saskaņā ar šo pantu, ja saņemtajā atbildē, kura minēta Regulas (ES) 2019/817 22. panta 2. punktā, ir norādīts, ka dati tiek glabāti *ETIAS* centrālajā sistēmā glabātajās pieteikuma datnēs.";

11) regulas 53. pantā iekļauj šādu punktu:

"1.a Gadījumos, kad Eiropols ir veicis vaicājumu *CIR* saskaņā ar Regulas (ES) 2019/817 22. pantu, datu aplūkošanas nolūkā tas var piekļūt pieteikuma datnēm, ko *ETIAS* centrālajā sistēmā glabā saskaņā ar šo pantu, ja saņemtajā atbildē, kura minēta Regulas (ES) 2019/817 22. panta 2. punktā, ir norādīts, ka dati tiek glabāti *ETIAS* centrālajā sistēmā glabātajās pieteikuma datnēs.";

12) regulas 65. panta 3. punkta piektajā daļā vārdus "17. panta 2. punkta a), b), d), e) un f) apakšpunktā" aizstāj ar vārdiem "17. panta 2. punkta a), aa), b), d), e) un f) apakšpunktā";

13) regulas 69. panta 1. punktā iekļauj šādu apakšpunktu:

"ca) vajadzības gadījumā atsauci uz *ESP* meklēšanas portāla izmantošanu, lai veiktu vaicājumu *ETIAS* centrālajā sistēmā, kā minēts Regulas (ES) 2019/817 7. panta 2. punktā,";

14) regulas 73. panta 2. punktā vārdus "centrālais datu repozitorijs" aizstāj ar vārdiem "Regulas (ES) 2019/817 39. pantā minētais centrālais ziņošanas un statistikas repozitorijs, ciktāl tajā ir ietverti dati, kas iegūti no *ETIAS* centrālās sistēmas saskaņā ar šīs regulas 84. pantu";

15) regulas 74. panta 1. punkta pirmo daļu aizstāj ar šādu:

"1. Pēc *ETIAS* darbības sākuma *eu-LISA* ir atbildīga par *ETIAS* centrālās sistēmas un NUI tehnisko pārvaldību. Tā arī atbild par jebkādu tehnisku testēšanu, kas nepieciešama, lai izveidotu un atjauninātu *ETIAS* pārbaudes noteikumus. Sadarbībā ar dalībvalstīm tā nodrošina, ka vienmēr tiek izmantota labākā pieejamā tehnoloģija, ņemot vērā izmaksu un ieguvumu analīzi. *eu-LISA* ir arī atbildīga par komunikāciju infrastruktūras tehnisko pārvaldību starp *ETIAS* centrālo sistēmu un NUI, kā arī par publisko tīmekļa vietni, lietotni mobilajām ierīcēm, e-pasta pakalpojumu, droša konta pakalpojumu, pieteikuma iesniedzējiem paredzētu pārbaudes rīku, pieteikuma iesniedzējiem paredzētu piekrišanas rīku, *ETIAS* kontrolsarakstam paredzētu novērtēšanas rīku, pārvadātāju vārteju, tīmekļa pakalpojumu un pieteikumu apstrādes programmatūru.";

16) regulas 84. panta 2. punkta pirmo daļu aizstāj ar šādu:

"2. Šā panta 1. punkta nolūkā *eu-LISA* glabā 1. punktā minētos datus centrālajā ziņošanas un statistikas repozitorijā, kas minēts Regulas (ES) 2019/817 39. pantā. Saskaņā ar minētās regulas 39. panta 1. punktu vairākas sistēmas aptveroši statistikas dati un analītiski ziņojumi ļauj šā panta 1. punktā uzskaitītajām iestādēm iegūt pielāgojamus pārskatus un statistikas datus, atbalstīt 33. pantā minēto *ETIAS* pārbaudes noteikumu īstenošanu, uzlabot novērtējumu par drošības, nelikumīgas imigrācijas un augstiem epidēmijas riskiem, palielināt robežpārbaužu efektivitāti un palīdzēt *ETIAS* centrālajai vienībai un *ETIAS* valsts vienībām apstrādāt ceļošanas atļauju pieteikumus.";

17) regulas 84. panta 4. punktam pievieno šādu daļu:

"Katras dienas statistikas datus glabā centrālajā ziņošanas un statistikas repozitorijā, kas minēts Regulas (ES) 2019/817 39. pantā."

62. pants

Grozījumi Regulā (ES) 2018/1726

Regulu (ES) 2018/1726 groza šādi:

1) regulas 12. pantu aizstāj ar šādu:

"*12. pants*

Datu kvalitāte

1. Neskarot dalībvalstu pienākumus attiecībā uz datiem, kas ievadīti sistēmās, kuru darbības pārvaldība ir aģentūras atbildībā, visām sistēmām, kuru darbības pārvaldība ir aģentūras atbildībā, aģentūra, cieši iesaistot padomdevēju grupas, iedibina automatizētus datu kvalitātes kontroles mehānismus un procedūras, vienotus datu kvalitātes rādītājus un minimālos datu glabāšanas kvalitātes standartus saskaņā ar attiecīgajiem noteikumiem, kas izklāstīti tiesību instrumentos, kuri reglamentē minētās informācijas sistēmas, un Eiropas Parlamenta un Padomes Regulu (ES) 2019/817 (*) un (ES) 2019/818 (**) 37. pantā.

2. Aģentūra saskaņā ar Regulas (ES) 2019/817 un Regulas (ES) 2019/818 39. pantu izveido centrālu ziņošanas un statistikas repozitoriju, kurā ir tikai anonimizēti dati, ievērojot konkrētus to tiesību instrumentu noteikumus, kas reglamentē aģentūras pārvaldīto lielapjoma IT sistēmu izstrādi, izveidi, darbību un izmantošanu.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).

(**) Eiropas Parlamenta un Padomes Regula (ES) 2019/818 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai policijas un tiesu iestāžu sadarbības, patvēruma un migrācijas jomā un groza Regulas (ES) 2018/1726, (ES) 2018/1862 un (ES) 2019/816 (OV L 135, 22.5.2019., 85. lpp.).";

2) regulas 19. panta 1. punktu groza šādi:

a) iekļauj šādu apakšpunktu:

"eea) pieņem ziņojumus par stāvokli sadarbspējas komponentu izstrādē saskaņā ar Regulas (ES) 2019/817 78. panta 2. punktu un Regulas (ES) 2019/818 74. panta 2. punktu.";

b) punkta ff) apakšpunktu aizstāj ar šādu:

"ff) pieņem ziņojumus par *SIS* tehnisko darbību saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1861 (*) 60. panta 7. punktu un Eiropas Parlamenta un Padomes Regulas (ES) 2018/1862 (**) 74. panta 8. punktu, par VIS tehnisko darbību saskaņā ar Regulas (EK) Nr. 767/2008 50. panta 3. punktu un Lēmuma 2008/633/TI 17. panta 3. punktu, par IIS tehnisko darbību saskaņā ar Regulas (ES) 2017/2226 72. panta 4. punktu, par *ETIAS* tehnisko darbību saskaņā ar Regulas (ES) 2018/1240 92. panta 4. punktu, par *ECRIS-TCN* tehnisko darbību un ECRIS ieteicamo īstenošanu saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/816 (***) 36. panta 8. punktu un par sadarbspējas komponentu tehnisko darbību saskaņā ar Regulas (ES) 2019/817 78. panta 3. punktu un Regulas (ES) 2019/818 74. panta 3. punktu;

(*) Eiropas Parlamenta un Padomes Regula (ES) 2018/1861 (2018. gada 28. novembris) 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 312, 7.12.2018., 14. lpp.).

(**) Eiropas Parlamenta un Padomes Regula (ES) 2018/1862 (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 (OV L 312, 7.12.2018., 56. lpp.).

(***) Eiropas Parlamenta un Padomes Regula (ES) 2019/816 (2019. gada 17. aprīlis), ar ko Eiropas Sodāmības reģistru informācijas sistēmas papildināšanai un atbalstam izveido centralizētu sistēmu (*ECRIS-TCN*) tādu dalībvalstu identificēšanai, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un ar ko groza Regulu (ES) 2018/1726 (OV L 135, 22.5.2019., 1. lpp.)";

c) punkta hh) apakšpunktu aizstāj ar šādu:

"hh) pieņem oficiālus komentārus par Eiropas Datu aizsardzības uzraudzītāja ziņojumiem par revīzijām saskaņā ar Regulas (ES) 2018/1861 56. panta 2. punktu, Regulas (EK) Nr. 767/2008 42. panta 2. punktu, Regulas (ES) Nr. 603/2013 31. panta 2. punktu, Regulas (ES) 2017/2226 56. panta 2. punktu, Regulas (ES) 2018/1240 67. pantu, Regulas (ES) 2019/816 29. panta 2. punktu un Regulu (ES) 2019/817 un (ES) 2019/818 52. pantu un nodrošina atbilstošus pēcpasākumus pēc šīm revīzijām;";

d) panta mm) apakšpunktu aizstāj ar šādu:

"mm) nodrošina, ka ik gadu publicē tādu kompetento iestāžu sarakstu, kas ir pilnvarotas veikt *SIS* iekļauto datu tiešu meklēšanu saskaņā ar Regulas (ES) 2018/1861 41. panta 8. punktu un Regulas (ES) 2018/1862 56. panta 7. punktu, kā arī *SIS* valstu sistēmu biroju (N.*SIS* biroji) un *SIRENE* biroju sarakstu, kā minēts attiecīgi Regulas (ES) 2018/1861 7. panta 3. punktā un Regulas (ES) 2018/1862 7. panta 3. punktā, kā arī kompetento iestāžu sarakstu saskaņā ar Regulas (ES) 2017/2226 65. panta 2. punktu, kompetento iestāžu sarakstu saskaņā ar Regulas (ES) 2018/1240 87. panta 2. punktu, centrālo iestāžu sarakstu saskaņā ar Regulas (ES) 2019/816 34. panta 2. punktu un iestāžu sarakstu saskaņā ar Regulas (ES) 2019/817 71. panta 1. punktu un Regulas (ES) 2019/818 67. panta 1. punktu;";

3) regulas 22. panta 4. punktu aizstāj ar šādu:

"4. Eiropols un *Eurojust* drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par *SIS* II saistībā ar Lēmuma 2007/533/TI piemērošanu.

Eiropas Robežu un krasta apsardzes aģentūra drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par *SIS* saistībā ar Regulas (ES) 2016/1624 piemērošanu.

Eiropols drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par VIS saistībā ar Lēmuma 2008/633/TI piemērošanu vai jautājums par *Eurodac* saistībā ar Regulas (ES) Nr. 603/2013 piemērošanu.

Eiropols drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par IIS saistībā ar Regulas (ES) 2017/2226 piemērošanu vai ja darba kārtībā ir jautājums par *ETIAS* saistībā ar Regulas (ES) 2018/1240 piemērošanu.

Eiropas Robežu un krasta apsardzes aģentūra arī drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par *ETIAS* saistībā ar Regulas (ES) 2018/1240 piemērošanu.

Eiropols, *Eurojust* un Eiropas Prokuratūra arī drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par Regulu (ES) 2019/816.

Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra arī drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par Regulām (ES) 2019/817 un (ES) 2019/818.

Valde uz savām sanāksmēm novērotāja statusā var uzaicināt jebkuru citu personu, kuras viedoklis to varētu interesēt.";

4) regulas 24. panta 3. punkta p) apakšpunktu aizstāj ar šādu:

"p) to, lai, neskarot Civildienesta noteikumu 17. pantu, tiktu noteiktas konfidencialitātes prasības ar mērķi panākt atbilstību Regulas (EK) Nr. 1987/2006 17. pantam, Lēmuma 2007/533/TI 17. pantam, Regulas (EK) Nr. 767/2008 26. panta 9. punktam, Regulas (ES) Nr. 603/2013 4. panta 4. punktam, Regulas (ES) 2017/2226 37. panta 4. punktam, Regulas (ES) 2018/1240 74. panta 2. punktam, Regulas (ES) 2019/816 11. panta 16. punktam un Regulu (ES) 2019/817 un (ES) 2019/818 55. panta 2. punktam;";

5) regulas 27. pantu groza šādi:

a) panta 1. punktā iekļauj šādu apakšpunktu:

"da) padomdevēju grupa sadarbspējas jautājumos;";

b) panta 3. punktu aizstāj ar šādu:

"3. Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra var iecelt katrs savu pārstāvi *SIS* II padomdevēju grupā.

Eiropols var iecelt vienu pārstāvi arī VIS un *Eurodac*, un IIS-*ETIAS* padomdevēju grupās.

Eiropas Robežu un krasta apsardzes aģentūra arī var iecelt vienu pārstāvi IIS-*ETIAS* padomdevēju grupā.

Eurojust, Eiropols un Eiropas Prokuratūra var katrs iecelt vienu pārstāvi *ECRIS-TCN* padomdevēju grupā.

Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra var iecelt katrs savu pārstāvi padomdevēju grupā sadarbspējas jautājumos."

63. pants

Grozījumi Regulā (ES) 2018/1861

Regulu (ES) 2018/1861 groza šādi:

1) regulas 3. pantam pievieno šādus punktus:

"22) "*ESP*" ir Eiropas meklēšanas portāls, kas izveidots ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/817 (*) 6. panta 1. punktu;

23) "kopējais *BMS*" ir kopējais biometrisko datu salīdzināšanas pakalpojums, kas izveidots ar Regulas (ES) 2019/817 12. panta 1. punktu;

24) "*CIR*" ir kopējais identitātes repozitorijs, kas izveidots ar Regulas (ES) 2019/817 17. panta 1. punktu;

25) "*MID*" ir vairāku identitāšu detektors, kas izveidots ar Regulas (ES) 2019/817 25. panta 1. punktu.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).";

2) regulas 4. pantu groza šādi:

a) panta 1. punkta b) un c) apakšpunktu aizstāj ar šādiem:

"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*;

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; un

d) droša komunikāciju infrastruktūra starp CS-*SIS* un *ESP*, kopējā *BMS* un *MID* centrālajām infrastruktūrām.";

b) pievieno šādus punktus:

"8. Neskarot šā panta 1. līdz 5. punktu, *SIS* datus var arī meklēt, izmantojot *ESP*.

9. Neskarot šā panta 1. līdz 5. punktu, *SIS* datus var arī nosūtīt, izmantojot drošo komunikāciju infrastruktūru, kas minēta 1. punkta d) apakšpunktā. Šī nosūtīšana nepārsniedz apjomu, kādā dati ir vajadzīgi Regulas (ES) 2019/817 nolūkiem.";

3) regulas 7. pantā iekļauj šādu punktu:

"2.a *SIRENE* biroji arī nodrošina atšķirīgu identitāšu manuālu verifikāciju saskaņā ar Regulas (ES) 2019/817 29. pantu. Ciktāl tas ir nepieciešams šā uzdevuma veikšanai, *SIRENE* birojiem ir piekļuve datiem, kurus glabā *CIR* un *MID*, Regulas (ES) 2019/817 21. un 26. pantā paredzētajos nolūkos.";

4) regulas 12. panta 1. punktu aizstāj ar šādu:

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

Dalībvalstis nodrošina, ka katra piekļuve personas datiem, izmantojot *ESP*, arī tiek ierakstīta, lai varētu pārbaudīt, vai meklēšana bija likumīga, lai uzraudzītu datu apstrādes likumību, pašuzraudzības nolūkos un lai nodrošinātu datu integritāti un drošību.";

5) regulas 34. panta 1. punktam pievieno šādu apakšpunktu:

"g) pārbaudītu atšķirīgās identitātes un apkarotu identitātes viltošanu saskaņā ar Regulas (ES) 2019/817 V nodaļu.";

6) regulas 60. panta 6. punktu aizstāj ar šādu:

"6. Šīs regulas 15. panta 4. punkta un šā panta 3., 4. un 5. punkta nolūkos datus, kuri minēti 15. panta 4. punktā un šā panta 3. punktā un kuri neļauj identificēt personas, *eu-LISA* glabā centrālajā ziņošanas un statistikas repozitorijā, kas minēts Regulas (ES) 2019/817 39. pantā.

eu-LISA ļauj Komisijai un šā panta 5. punktā minētajām struktūrām iegūt pēc pasūtījuma sagatavotus ziņojumus un statistiku. Pēc pieprasījuma *eu-LISA* piešķir dalībvalstīm, Komisijai, Eiropolam un Eiropas Robežu un krasta apsardzes aģentūrai piekļuvi centrālajam ziņošanas un statistikas repozitorijam saskaņā ar Regulas (ES) 2019/817 39. pantu."

64. pants

Grozījumi Lēmumā 2004/512/EK

Lēmuma 2004/512/EK 1. panta 2. punktu aizstāj ar šādu:

"2. Vīzu informācijas sistēmas pamatā ir centralizēta arhitektūra, un to veido:

a) kopējā identitātes repozitorija centrālā infrastruktūra, kā minēts Eiropas Parlamenta un Padomes Regulas (ES) 2019/817 (*) 17. panta 2. punkta a) apakšpunktā;

b) centrāla informācijas sistēma, turpmāk "Centrālā vīzu informācijas sistēma" (CS-VIS);

c) saskarne katrā dalībvalstī, turpmāk "valsts saskarne" (NI-VIS), kas nodrošina savienojumu ar attiecīgās dalībvalsts atbilstīgo centrālo valsts iestādi;

d) komunikācijas infrastruktūra starp Centrālo vīzu informācijas sistēmu un valsts saskarnēm;

e) drošs sakaru kanāls starp IIS centrālo sistēmu un CS-VIS;

f) droša komunikāciju infrastruktūra starp VIS centrālo sistēmu un Eiropas meklēšanas portāla, kas izveidots ar Regulas (ES) 2019/817 6. panta 1. punktu, un kopējā identitātes repozitorija, kas izveidots ar Regulas (ES) 2019/817 17. panta 1. punktu, centrālajām infrastruktūrām.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.)."

65. pants

Grozījumi Lēmumā 2008/633/TI

Lēmumu 2008/633/TI groza šādi:

1) lēmuma 5. pantā iekļauj šādu punktu:

"1.a Gadījumos, kad izraudzītās iestādes ir veikušas vaicājumu kopējā identitātes repozitorijā (*CIR*) saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/817 (*) 22. pantu, tās var piekļūt VIS datu aplūkošanai, ja ir izpildīti šajā pantā paredzētie piekļuves nosacījumi un ja saņemtajā atbildē, kas minēta Regulas 22. panta 2. punktā, ir norādīts, ka dati tiek glabāti VIS.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).";

2) lēmuma 7. pantā iekļauj šādu jaunu punktu:

"1.a Gadījumos, kad Eiropols ir veicis vaicājumu *CIR* saskaņā ar Regulas (ES) 2019/817 22. pantu, Eiropols var piekļūt VIS datu aplūkošanai, ja ir izpildīti šajā pantā paredzētie nosacījumi un ja saņemtajā atbildē, kas minēta minētās Regulas 22. panta 2. punktā, ir norādīts, ka dati tiek glabāti VIS."

X NODAĻA

Nobeiguma noteikumi

66. pants

Ziņošana un statistika

1. Dalībvalstu kompetento iestāžu, Komisijas un *eu-LISA* pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai tikai ziņošanas un statistikas nolūkos aplūkotu šādus datus, kas saistīti ar *ESP*:

a) vaicājumu skaits pa katru *ESP* profila lietotāju;

b) vaicājumu skaits pa katru Interpola datubāzi.

No datiem nav iespējams identificēt personas.

2. Dalībvalstu kompetento iestāžu, Komisijas un *eu-LISA* pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai tikai ziņošanas un statistikas nolūkos aplūkotu šādus datus, kas saistīti ar *CIR*:

a) vaicājumu skaits 20., 21. un 22. panta nolūkos;

b) personas valstspiederība, dzimums un dzimšanas gads;

c) ceļošanas dokumenta veids un izdevējas valsts trīs burtu kods;

d) to meklējumu skaits, kuri veikti, izmantojot un neizmantojot biometriskos datus.

No datiem nav iespējams identificēt personas.

3. Dalībvalstu kompetento iestāžu, Komisijas un *eu-LISA* pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai tikai ziņošanas un statistikas nolūkos aplūkotu šādus datus, kas saistīti ar *MID*:

a) to meklējumu skaits, kuri veikti, izmantojot un neizmantojot biometriskos datus;

b) katra veida saikņu skaits un tās ES informācijas sistēmas, kuras satur saistītos datus;

c) laikposms, kurā dzeltenā vai sarkanā saikne tika saglabāta sistēmā.

No datiem nav iespējams identificēt personas.

4. Eiropas Robežu un krasta apsardzes aģentūras pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai aplūkotu šā panta 1., 2. un 3. punktā minētos datus nolūkā veikt riska analīzi un neaizsargātības novērtējumus, kā minēts minētās Eiropas Parlamenta un Padomes Regulas (ES) 2016/1624 ([40]) 11. un 13. pantā.

5. Eiropola pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai aplūkotu šā panta 2. un 3. punktā minētos datus nolūkā veikt stratēģisko, tematisko un operatīvo analīzi, kā minēts Regulas (ES) 2016/794 18. panta 2. punkta b) un c) apakšpunktā.

6. Šā panta 1., 2. un 3. punkta nolūkā *eu-LISA* glabā minētajos punktos minētos datus *CRRS*. No *CRRS* iekļautajiem datiem nav iespējams identificēt personas, bet dati ļauj šā panta 1., 2. un 3. punktā uzskaitītajām iestādēm iegūt pielāgojamus pārskatus un statistiku, lai palielinātu robežpārbaužu efektivitāti, palīdzētu iestādēm apstrādāt vīzas pieteikumus un atbalstītu Savienībā uz faktiem pamatotas politikas veidošanu migrācijas un drošības jomā.

7. Komisija pēc pieprasījuma dara Eiropas Savienības Pamattiesību aģentūrai pieejamu attiecīgu informāciju, lai tā izvērtētu šīs regulas ietekmi uz pamattiesībām.

67. pants

Pārejas periods Eiropas meklēšanas portāla izmantošanai

1. Divu gadu laikposmā no *ESP* darbības uzsākšanas nepiemēro 7. panta 2. un 4. punktā minētos pienākumus, un *ESP* izmantošana nav obligāta.

2. Komisija tiek pilnvarota pieņemt deleģēto aktu saskaņā ar 73. pantu, lai grozītu šo regulu, pagarinot šā panta 1. punktā minēto laikposmu vienu reizi uz laiku, kas nepārsniedz vienu gadu, ja *ESP* īstenošanas novērtējums liecina, ka šāds pagarinājums ir nepieciešams, īpaši ņemot vērā ietekmi, kādu *ESP* ieviešana radītu attiecībā uz robežpārbaužu organizāciju un ilgumu.

68. pants

Pārejas periods, ko piemēro noteikumiem par piekļuvi kopējam identitātes repozitorijam nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus

Šīs regulas 22. pantu, 60. panta 8. un 9. punktu, 61. panta 10. un 11. punktu un 65. pantu piemēro no *CIR* darbības uzsākšanas dienas, kas minēta 72. panta 3. punktā.

([40]) 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.).

69. pants

Pārejas periods vairāku identitāšu konstatēšanai

1. Viena gada laikposmā pēc tam, kad *eu-LISA* ir paziņojusi par 72. panta 4. punkta b) apakšpunktā minētā *MID* testa pabeigšanu, un pirms *MID* darbības uzsākšanas *ETIAS* centrālā vienība ir atbildīga par to, lai veiktu vairāku identitāšu konstatēšanu, izmantojot IIS, VIS, *Eurodac* un *SIS* glabātos datus. Vairāku identitāšu konstatēšanu veic, izmantojot vienīgi biometriskos datus.

2. Ja vaicājums uzrāda vienu vai vairākas atbilstības un identitātes dati saistītajās datnēs ir vienādi vai līdzīgi, izveido baltu saikni saskaņā ar 33. pantu.

Ja vaicājums uzrāda vienu vai vairākas atbilstības un identitātes datus saistītajās datnēs nevar uzskatīt par līdzīgiem, izveido dzeltenu saikni saskaņā ar 30. pantu un piemēro 29. pantā minēto procedūru.

Ja tiek uzrādītas vairākas atbilstības, izveido saikni starp katru datu vienību, kas izraisa atbilstību.

3. Ja ir izveidota dzeltena saikne, *MID* piešķir *ETIAS* centrālajai vienībai piekļuvi dažādās ES informācijas sistēmās esošajiem identitātes datiem.

4. Ja ir izveidota saikne uz tādu brīdinājumu *SIS*, kas nav brīdinājums, kurš izveidots saskaņā ar Regulas (ES) 2018/1860 3. pantu, Regulas (ES) 2018/1861 24. un 25. pantu vai Regulas (ES) 2018/1862 38. pantu, *MID* piešķir brīdinājumu izveidojušās dalībvalsts *SIRENE* birojam piekļuvi dažādās informācijas sistēmās esošajiem identitātes datiem.

5. *ETIAS* centrālajai vienībai vai šā panta 4. punktā minētajos gadījumos - tās dalībvalsts *SIRENE* birojam, kura izveidoja brīdinājumu, ir piekļuve identitātes apstiprinājuma datnē ietvertajiem datiem, un tie novērtē atšķirīgās identitātes un atjaunina saikni saskaņā ar 31., 32. un 33. pantu, un pievieno to identitātes apstiprinājuma datnei.

6. *ETIAS* centrālā vienība Komisijai saskaņā ar 71. panta 3. punktu paziņo tikai tad, kad visas dzeltenās saiknes ir manuāli verificētas un to statuss atjaunināts, pārveidojot tās par zaļajām, baltajām vai sarkanajām saiknēm.

7. Dalībvalstis vajadzības gadījumā palīdz *ETIAS* centrālajai vienībai veikt vairāku identitāšu konstatēšanu atbilstīgi šim pantam.

8. Komisija tiek pilnvarota pieņemt deleģētu aktu saskaņā ar 73. pantu, lai grozītu šo regulu, pagarinot šā panta 1. punktā minēto laikposmu par sešiem mēnešiem, ko var atjaunot divas reizes, katru reizi uz sešiem mēnešiem. Šādu pagarinājumu piešķir tikai pēc vairāku identitāšu konstatēšanas pabeigšanas laika novērtējuma saskaņā ar šo pantu, ja tas liecina, ka vairāku identitāšu konstatēšanu nevar pabeigt pirms 1. punktā minētā laikposma vai jebkura pastāvoša pagarinājuma beigām no *ETIAS* centrālās vienības neatkarīgu apstākļu dēļ un ja nav iespējams piemērot korektīvus pasākumus. Novērtējumu veic ne vēlāk kā trīs mēnešus pirms šāda laikposma vai pastāvoša pagarinājuma beigām.

70. pants

Izmaksas

1. Izmaksas, kas rodas saistībā ar *ESP*, kopējā *BMS*, *CIR* un *MID* izveidi un darbību, sedz no Savienības vispārējā budžeta.

2. Izmaksas, kas rodas saistībā ar esošo valsts infrastruktūru integrāciju un šo infrastruktūru savienojumu ar valsts vienotajām saskarnēm, kā arī ar valsts vienoto saskarņu mitināšanu, sedz no Savienības vispārējā budžeta.

Netiek iekļautas šādas izmaksas:

a) dalībvalstu projektu vadības birojs (sanāksmes, komandējumi, biroji);

b) valstu IT sistēmu mitināšana (telpas, īstenošana, elektroenerģija, dzesēšana);

c) valstu IT sistēmu ekspluatācija (operatori un atbalsta līgumi);

d) valstu komunikācijas tīklu plānošana, izstrāde, ieviešana, ekspluatācija un uzturēšana.

3. Lai segtu šīs regulas īstenošanas izmaksas, kā paredzēts šā panta 1. un 2. punktā, neskarot šā mērķa turpmāku finansēšanu no citiem Eiropas Savienības vispārējā budžeta avotiem, tiek piesaistīti 32 077 000 EUR no Regulas (ES) Nr. 515/2014 5. panta 5. punkta b) apakšpunktā paredzētajiem 791 000 000 EUR.

4. No 3. punktā minētajiem finanšu līdzekļiem 22 861 000 EUR piešķir *eu-LISA*, 9 072 000 EUR piešķir Eiropolam un 144 000 EUR piešķir Eiropas Savienības Tiesībaizsardzības apmācības aģentūrai (*CEPOL*), lai atbalstītu šīs aģentūras to attiecīgo uzdevumu izpildē atbilstīgi šai regulai. Šādu finansējumu īsteno ar netiešo pārvaldību.

5. Izmaksas, kas rodas izraudzītajām iestādēm, sedz attiecīgi izraudzītājas dalībvalstis. Izmaksas par katras izraudzītās iestādes savienojumu ar *CIR* sedz katra dalībvalsts.

Izmaksas, kas rodas Eiropolam, tostarp par savienojumu ar *CIR*, sedz Eiropols.

71. pants

Paziņojumi

1. Dalībvalstis paziņo *eu-LISA* par iestādēm, kuras minētas 7., 20., 21. un 26. pantā un kuras attiecīgi var izmantot *ESP*, *CIR* un *MID* vai kurām ir piekļuve tiem.

Minēto iestāžu konsolidētu sarakstu publicē *Eiropas Savienības Oficiālajā Vēstnesī* trīs mēnešu laikā no dienas, kad katrs sadarbspējas komponents ir uzsācis darbību saskaņā ar 72. pantu. Ja sarakstā ievieš grozījumus, *eu-LISA* reizi gadā publicē atjauninātu konsolidētu sarakstu.

2. *eu-LISA* paziņo Komisijai par 72. panta 1. punkta b) apakšpunktā, 2. punkta b) apakšpunktā, 3. punkta b) apakšpunktā, 4. punkta b) apakšpunktā, 5. punkta b) apakšpunktā un 6. punkta b) apakšpunktā minētā testa sekmīgu pabeigšanu.

3. *ETIAS* centrālā vienība paziņo Komisijai par 69. pantā paredzētā pārejas perioda sekmīgu pabeigšanu.

4. Komisija dara saskaņā ar 1. punktu paziņoto informāciju pieejamu dalībvalstīm un sabiedrībai, izmantojot publisku tīmekļa vietni, kura pastāvīgi tiek atjaunināta.

72. pants

Darbības sākums

1. Komisija ar īstenošanas aktu nosaka dienu, no kuras *ESP* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 8. panta 2. punktā, 9. panta 7. punktā un 43. panta 5. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *ESP* tests, ko *eu-LISA* ir veikusi, sadarbojoties ar dalībvalstu iestādēm un Savienības aģentūrām, kas var lietot *ESP*;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 8. panta 1. punktā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

ESP veic vaicājumus Interpola datubāzēs tikai tad, ja tehniskie pasākumi ļauj nodrošināt atbilstību 9. panta 5. punktam. Ja nav iespējams nodrošināt atbilstību 9. panta 5. punktam, *ESP* neveic vaicājumus Interpola datubāzēs, bet tas neaizkavē *ESP* darbības sākumu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

2. Komisija ar īstenošanas aktu nosaka dienu, no kuras kopējais *BMS* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 13. panta 5. punktā un 43. panta 5. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs kopējā *BMS* tests, ko tā veikusi, sadarbojoties ar dalībvalstu iestādēm;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 13. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

d) *eu-LISA* ir paziņojusi Komisijai par 5. punkta b) apakšpunktā minētā testa sekmīgu pabeigšanu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

3. Komisija ar īstenošanas aktu nosaka dienu, no kuras *CIR* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 43. panta 5. punktā un 78. panta 10. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *CIR* tests, ko tā veikusi, sadarbojoties ar dalībvalstu iestādēm;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 18. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

d) *eu-LISA* ir paziņojusi Komisijai par 5. punkta b) apakšpunktā minētā testa sekmīgu pabeigšanu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

4. Komisija ar īstenošanas aktu nosaka dienu, no kuras *MID* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 28. panta 5. un 7. punktā, 32. panta 5. punktā, 33. panta 6. punktā, 43. panta 5. punktā un 49. panta 6. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *MID* tests, ko tā veikusi, sadarbojoties ar dalībvalstu iestādēm un *ETIAS* centrālo vienību;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 34. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

d) *ETIAS* centrālā vienība ir paziņojusi Komisijai saskaņā ar 71. panta 3. punktu;

e) *eu-LISA* ir paziņojusi Komisijai par 1. punkta b) apakšpunktā, 2. punkta b) apakšpunktā, 3. punkta b) apakšpunktā un 5. punkta b) apakšpunktā minēto testu sekmīgu pabeigšanu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

5. Komisija ar īstenošanas aktiem nosaka dienu, no kuras sāk izmantot automatizētos datu kvalitātes kontroles mehānismus un procedūras, kopējos datu kvalitātes indikatorus un datu kvalitātes minimālos standartus, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 37. panta 4. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs automatizēto datu kvalitātes kontroles mehānismu un procedūru, kopējo datu kvalitātes indikatoru un datu kvalitātes minimālo standartu tests, ko tā veikusi, sadarbojoties ar dalībvalstu iestādēm.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

6. Komisija ar īstenošanas aktu nosaka dienu, no kuras *CRRS* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 39. panta 5. punktā un 43. panta 5. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *CRRS* tests, ko tā veikusi, sadarbojoties ar dalībvalstu iestādēm;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 39. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

7. Komisija informē Eiropas Parlamentu un Padomi par saskaņā ar 1. punkta b) apakšpunktu, 2. punkta b) apakšpunktu, 3. punkta b) apakšpunktu, 4. punkta b) apakšpunktu, 5. punkta b) apakšpunktu un 6. punkta b) apakšpunktu veikto testu rezultātiem.

8. Dalībvalstis, *ETIAS* centrālā vienība un Eiropols sāk izmantot katru no sadarbspējas komponentiem no dienas, ko Komisija noteikusi attiecīgi saskaņā ar 1., 2., 3. un 4. punktu.

73. pants

Deleģēšanas īstenošana

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

2. Pilnvaras pieņemt 28. panta 5. punktā, 39. panta 5. punktā, 49. panta 6. punktā, 67. panta 2. punktā un 69. panta 8. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no 2019. gada 11. jūnija. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms piecu gadu laikposma beigām. Pilnvaru deleģēšana tiek automātiski pagarināta uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 28. panta 5. punktā, 39. panta 5. punktā, 49. panta 6. punktā, 67. panta 2. punktā un 69. panta 8. 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 28. panta 5. punktu, 39. panta 5. punktu, 49. panta 6. punktu, 67. panta 2. punktu un 69. panta 8. 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.

74. 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.

Ja komiteja atzinumu nesniedz, Komisija īstenošanas akta projektu nepieņem, un tiek piemērota Regulas (ES) Nr. 182/2011 5. panta 4. punkta trešā daļa.

75. pants

Padomdevēju grupa

eu-LISA izveido Sadarbspējas padomdevēju grupu. Sadarbspējas komponentu plānošanas un izstrādes posmā piemēro 54. panta 4., 5. un 6. punktu.

76. pants

Apmācība

Saskaņā ar Regulu (ES) 2018/1726 *eu-LISA* veic uzdevumus, kas saistīti ar apmācības sniegšanu par sadarbspējas komponentu tehnisko izmantošanu.

Dalībvalstu iestādes un Savienības aģentūras nodrošina saviem darbiniekiem, kas ir pilnvaroti apstrādāt datus, izmantojot sadarbspējas komponentus, atbilstīgas apmācības programmas par datu drošību, datu kvalitāti, datu aizsardzības noteikumiem, datu apstrādei piemērojamām procedūrām un pienākumiem sniegt informāciju saskaņā ar 32. panta 4. punktu, 33. panta 4. punktu un 47. pantu.

Attiecīgā gadījumā par minētajām tēmām organizē kopīgus mācību kursus Savienības līmenī, lai uzlabotu sadarbību un apmainītos ar paraugpraksi starp dalībvalstu iestāžu un Savienības aģentūru darbiniekiem, kas ir pilnvaroti apstrādāt datus, izmantojot sadarbspējas komponentus. Īpašu uzmanību pievērš vairāku identitāšu konstatēšanas procesam, tostarp atšķirīgu identitāšu manuālai verifikācijai un ar to saistītajai vajadzībai uzturēt atbilstošus pamattiesību aizsardzības pasākumus.

77. pants

Praktiskā rokasgrāmata

Komisija, cieši sadarbojoties ar dalībvalstīm, *eu-LISA* un citām attiecīgām Savienības aģentūrām, dara pieejamu praktisku rokasgrāmatu par sadarbspējas komponentu īstenošanu un pārvaldību. Praktiskā rokasgrāmata sniedz tehniskas un operatīvas norādes, ieteikumus un paraugpraksi. Komisija praktisko rokasgrāmatu pieņem ieteikuma veidā.

78. pants

Uzraudzība un izvērtēšana

1. *eu-LISA* nodrošina, ka ir ieviestas procedūras, lai uzraudzītu sadarbspējas komponentu izstrādi un to savienošanu ar valsts vienoto saskarni, ņemot vērā ar plānošanu un izmaksām saistītos mērķus, un lai uzraudzītu sadarbspējas komponentu darbību, ņemot vērā mērķus, kas saistīti ar pakalpojuma tehniskajiem rezultātiem, izmaksu lietderību, drošību un kvalitāti.

2. Līdz 2019. gada 12. decembrim un turpmāk ik pēc sešiem mēnešiem komponentu izstrādes posma laikā *eu-LISA* iesniedz ziņojumu Eiropas Parlamentam un Padomei par aktuālo situāciju saistībā ar sadarbspējas komponentu izstrādi, kā arī to savienojumu ar valsts vienoto saskarni. Tiklīdz izstrāde ir pabeigta, Eiropas Parlamentam un Padomei iesniedz ziņojumu, kurā sīki izskaidrots, kā tika sasniegti mērķi, jo īpaši saistībā ar plānošanu un izmaksām, kā arī pamatotas jebkādas atšķirības.

3. Četrus gadus pēc katra sadarbspējas komponenta darbības uzsākšanas saskaņā ar 72. pantu un turpmāk ik pēc četriem gadiem *eu-LISA* iesniedz Eiropas Parlamentam, Padomei un Komisijai ziņojumu par sadarbspējas komponentu tehnisko darbību, tostarp to drošību.

4. Turklāt vienu gadu pēc katra *eu-LISA* izstrādātā ziņojuma Komisija sagatavo sadarbspējas komponentu vispārēju izvērtējumu, kas ietver:

a) novērtējumu par šīs regulas piemērošanu;

b) salīdzinājumā ar šīs regulas mērķiem sasniegto rezultātu analīzi un tās ietekmi uz pamattiesībām, tostarp jo īpaši novērtējumu par sadarbspējas komponentu ietekmi uz tiesībām uz nediskriminēšanu;

c) novērtējumu par tīmekļa portāla darbību, tostarp tīmekļa portāla lietošanu raksturojošos rādītājus un izpildīto pieprasījumu skaitu;

d) novērtējumu par sadarbspējas komponentu pamatojuma turpmāku derīgumu;

e) novērtējumu par sadarbspējas komponentu drošību;

f) novērtējumu par to, kā identifikācijas nolūkā izmanto *CIR*;

g) novērtējumu par to, kā *CIR* izmanto nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus;

h) novērtējumu par jebkādām sekām, tostarp nesamērīgu ietekmi uz satiksmes plūsmu robežšķērsošanas vietās un ietekmi uz Savienības vispārējo budžetu;

i) novērtējumu par meklējumiem Interpola datubāzēs, izmantojot *ESP*, tostarp informāciju par atbilstību skaitu Interpola datubāzēs un informāciju par visām atklātajām problēmām.

Vispārējā izvērtējumā atbilstīgi šā punkta pirmajai daļai iekļauj jebkādus nepieciešamos ieteikumus. Komisija izvērtēšanas ziņojumu nosūta Eiropas Parlamentam, Padomei, Eiropas Datu aizsardzības uzraudzītājam un Eiropas Savienības Pamattiesību aģentūrai.

5. Līdz 2020. gada 12. jūnijam un katru gadu pēc tam, kamēr vēl nav pieņemti 72. pantā minētie Komisijas īstenošanas akti, Komisija iesniedz ziņojumu Eiropas Parlamentam un Padomei par stāvokli sagatavošanas darbos šīs regulas pilnai īstenošanai. Minētajā ziņojumā iekļauj arī detalizētu informāciju par radītajām izmaksām un informāciju par jebkādiem riskiem, kas var ietekmēt kopējās izmaksas.

6. Divus gadus pēc *MID* darbības sākuma saskaņā ar 72. panta 4. punktu Komisija sagatavo analīzi par *MID* ietekmi uz tiesībām uz nediskriminēšanu. Pēc šā pirmā ziņojuma analīze par *MID* ietekmi uz tiesībām uz nediskriminēšanu ir daļa no šā panta 4. punkta b) apakšpunktā minētās analīzes.

7. Dalībvalstis un Eiropols sniedz *eu-LISA* un Komisijai informāciju, kas vajadzīga, lai izstrādātu 3. līdz 6. punktā minētos ziņojumus. Šī informācija neapdraud darba metodes, un tajā neietver informāciju, kas atklāj izraudzīto iestāžu avotus, darbiniekus vai izmeklēšanas.

8. *eu-LISA* sniedz Komisijai informāciju, kas vajadzīga, lai izstrādātu 4. punktā minēto vispārējo izvērtējumu.

9. Ievērojot valsts tiesību aktus par konfidenciālas informācijas publicēšanu un neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību un sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta valsts veikta izmeklēšana, katra dalībvalsts un Eiropols sagatavo gada ziņojumus par to, cik efektīva ir bijusi piekļuve *CIR* glabātajiem datiem, kas īstenota nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, un šajos ziņojumos iekļauj informāciju un statistikas datus par:

a) aplūkošanas konkrēto mērķi, ietverot teroristu nodarījuma vai cita smaga noziedzīga nodarījuma veidu;

b) pamatotajiem iemesliem, kas norādīti saistībā ar pamatotajām aizdomām, ka uz aizdomās turēto personu, nodarījuma izdarītāju vai cietušo attiecas Regula (ES) 2017/2226, Regula (EK) Nr. 767/2008 vai Regula (ES) 2018/1240;

c) pieprasījumu skaitu piekļuvei *CIR*, kuras nolūks ir novērst, atklāt un izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus;

d) to lietu skaitu un veidu, kurās ir bijusi sekmīga identifikācija;

e) informāciju par to, cik bieži bija vajadzīgi izņēmumi steidzamības gadījumos un cik bieži tie tika izmantoti, tostarp par gadījumiem, kad centrālā piekļuves punkta veiktajā *ex post* verifikācijā netika atzīts, ka šāds ārkārtas steidzamības gadījums pastāvēja.

Dalībvalstu un Eiropola sagatavotos gada ziņojumus nosūta Komisijai līdz nākamā gada 30. jūnijam.

10. Dalībvalstīm dara pieejamu tehnisku risinājumu, kura nolūks ir pārvaldīt 22. pantā minētos lietotāju piekļuves pieprasījumus un atvieglot informācijas vākšanu saskaņā ar šā panta 7. un 9. punktu nolūkā sagatavot minētajos punktos minētos ziņojumus un statistiku. Komisija pieņem īstenošanas aktus, nosakot tehniskā risinājuma specifikācijas. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 74. panta 2. punktā.

79. pants

Stāšanās spēkā un piemērošana

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

Šīs regulas noteikumus par *ESP* piemēro no dienas, ko Komisija noteikusi saskaņā ar 72. panta 1. punktu.

Šīs regulas noteikumus par kopējo *BMS* piemēro no dienas, ko Komisija noteikusi saskaņā ar 72. panta 2. punktu.

Šīs regulas noteikumus par *CIR* piemēro no dienas, ko Komisija noteikusi saskaņā ar 72. panta 3. punktu.

Šīs regulas noteikumus par *MID* piemēro no dienas, ko Komisija noteikusi saskaņā ar 72. panta 4. punktu.

Šīs regulas noteikumus par automatizētajiem datu kvalitātes kontroles mehānismiem un procedūrām, kopējiem datu kvalitātes indikatoriem un minimālajiem datu kvalitātes standartiem piemēro no dienas, ko Komisija noteikusi saskaņā ar 72. panta 5. punktu.

Šīs regulas noteikumus par *CRRS* piemēro no dienas, ko Komisija noteikusi saskaņā ar 72. panta 6. punktu.

Šīs regulas 6., 12., 17., 25., 38., 42., 54., 56., 57., 70., 71., 73., 74., 75. un 77. pantu un 78. panta 1. punktu piemēro no 2019. gada 11. jūnija.

Attiecībā uz *Eurodac* šo regulu piemēro no dienas, kad kļūst piemērojama Eiropas Parlamenta un Padomes Regulas (ES) Nr. 603/2013 pārstrādātā versija.

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

Briselē, 2019. gada 20. maijā

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*
A. TAJANI	G. CIAMBA

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2019/818

(2019. gada 20. maijs),

ar ko izveido satvaru ES informācijas sistēmu sadarbspējai policijas un tiesu iestāžu sadarbības, patvēruma un migrācijas jomā un groza Regulas (ES) 2018/1726, (ES) 2018/1862 un (ES) 2019/816

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16. panta 2. punktu, 74. pantu, 78. panta 2. punkta e) apakšpunktu, 79. panta 2. punkta c) apakšpunktu, 82. panta 1. punkta d) apakšpunktu, 85. panta 1. punktu, 87. panta 2. punkta a) apakšpunktu un 88. panta 2. punktu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu ([1]),

pēc apspriešanās ar Reģionu komiteju,

saskaņā ar parasto likumdošanas procedūru ([2]),

tā kā:

(1) Komisija 2016. gada 6. aprīļa paziņojumā "Spēcīgākas un viedākas robežu un drošības informācijas sistēmas" uzsvēra nepieciešamību uzlabot Savienības datu pārvaldības arhitektūru robežu pārvaldības un drošības jomā. Ar šo paziņojumu tika sākta virzība uz ES drošības, robežu un migrācijas pārvaldības informācijas sistēmu sadarbspējas panākšanu, lai novērstu ar šīm sistēmām saistītos strukturālos trūkumus, kas apgrūtina valsts iestāžu darbu, un nodrošinātu, ka robežsargu, muitas iestāžu, policijas darbinieku un tiesu iestāžu rīcībā ir nepieciešamā informācija.

(2) 2016. gada 6. jūnija Ceļvedī ar mērķi uzlabot informācijas apmaiņu un informācijas pārvaldību, tostarp sadarbspējas risinājumus, tieslietu un iekšlietu jomā Padome apzināja dažādas tiesiskas, tehniskas un operatīvas problēmas ES informācijas sistēmu sadarbspējā un aicināja rast atbilstošus risinājumus.

(3) 2016. gada 6. jūlija rezolūcijā par stratēģiskajām prioritātēm attiecībā uz Komisijas 2017. gada darba programmu ([3]) Eiropas Parlaments aicināja iesniegt priekšlikumus par pastāvošo informācijas sistēmu uzlabošanu un attīstīšanu, informācijas trūkumu novēršanu un šo sistēmu sadarbspējas panākšanu, kā arī priekšlikumus par obligāto informācijas apmaiņu ES, kuri papildināti ar nepieciešamajiem mehānismiem datu aizsardzībai.

(4) Eiropadome savos 2016. gada 15.decembra secinājumos aicināja turpināt darbu, lai izveidotu ES informācijas sistēmu un datubāzu sadarbspēju.

(5) Augsta līmeņa ekspertu grupa informācijas sistēmu un sadarbspējas jautājumos 2017. gada 11. maija galīgajā ziņojumā secināja, ka bija nepieciešams un tehniski iespējams sākt darbu pie praktiskiem sadarbspējas risinājumiem un ka principā sadarbspēja var gan sniegt operatīvos ieguvumus, gan to var izstrādāt atbilstīgi datu aizsardzības prasībām.

(6) 2017. gada 16. maija paziņojumā "Septītais progresa ziņojums virzībā uz efektīvu un patiesu drošības savienību" Komisija – saskaņā ar 2016. gada 6. aprīļa paziņojumu un ņemot vērā konstatējumus un ieteikumus, kurus izteikusi augsta līmeņa ekspertu grupa informācijas sistēmu un sadarbspējas jautājumos, – izklāstīja jaunu pieeju robežu, drošības un migrācijas datu pārvaldībai, saskaņā ar kuru visām ES informācijas sistēmām drošības, robežu un migrācijas pārvaldības jomā jābūt sadarbspējīgām, pilnībā ievērojot pamattiesības.

([1]) OV C 283, 10.8.2018., 48. lpp.
([2]) Eiropas Parlamenta 2019. gada 16. aprīļa nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2019. gada 14. maija lēmums.
([3]) OV C 101, 16.3.2018., 116. lpp.

(7) 2017. gada 9. jūnija secinājumos par turpmāko virzību ar mērķi uzlabot informācijas apmaiņu un nodrošināt ES informācijas sistēmu sadarbspēju Padome aicināja Komisiju rast sadarbspējas risinājumus, kā ierosinājusi augsta līmeņa ekspertu grupa.

(8) Eiropadome savos 2017. gada 23. jūnija secinājumos uzsvēra nepieciešamību uzlabot sadarbspēju starp datubāzēm un aicināja Komisiju cik drīz vien iespējams sagatavot tiesību akta projektu, pamatojoties uz priekšlikumiem, kurus izteikusi augsta līmeņa ekspertu grupa informācijas sistēmu un sadarbspējas jautājumos.

(9) Lai uzlabotu pārbaužu lietderību un efektivitāti pie ārējām robežām, palīdzētu novērst un apkarot nelikumīgu imigrāciju un sekmētu augsta drošības līmeņa nodrošināšanu Savienības brīvības, drošības un tiesiskuma telpā, tostarp sabiedriskās drošības un sabiedriskās kārtības uzturēšanu un drošības sargāšanu dalībvalstu teritorijās, uzlabotu kopējās vīzu politikas īstenošanu, palīdzētu starptautiskās aizsardzības pieteikumu izskatīšanā, palīdzētu novērst, atklāt un izmeklēt teroristu nodarījumus un citus smagus noziedzīgus nodarījumus, palīdzētu identificēt nezināmas personas, kuras nespēj sevi identificēt, vai neidentificētas mirstīgās atliekas dabas katastrofas, negadījuma vai teroristu uzbrukuma gadījumā un saglabātu sabiedrības uzticēšanos Savienības migrācijas un patvēruma sistēmai, Savienības drošības pasākumiem un Savienības spējām pārvaldīt ārējo robežu, būtu jāizveido sadarbspēja starp ES informācijas sistēmām, proti, ieceļošanas/izceļošanas sistēmu (IIS), vīzu informācijas sistēmu (VIS), Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*), *Eurodac*, Šengenas informācijas sistēmu (*SIS*) un Eiropas Sodāmības reģistru informācijas sistēmu trešo valstu valstspiederīgajiem (*ECRIS-TCN*), lai šīs ES informācijas sistēmas un to dati papildinātu cita citu, vienlaikus ievērojot personas pamattiesības, jo īpaši tiesības uz personas datu aizsardzību. Lai to panāktu, kā sadarbspējas komponenti būtu jāizveido Eiropas meklēšanas portāls (*ESP*), kopējs biometrisko datu salīdzināšanas pakalpojums (kopējais *BMS*), kopējs identitātes repozitorijs (*CIR*) un vairāku identitāšu detektors (*MID*).

(10) ES informācijas sistēmu sadarbspējai būtu jāļauj tām papildināt citai citu, lai atvieglotu personu, tostarp personu, kuras nespēj sevi identificēt, vai neidentificētu cilvēku mirstīgo atlieku, pareizu identifikāciju, palīdzētu apkarot identitātes viltošanu, uzlabotu un saskaņotu attiecīgo ES informācijas sistēmu prasības datu kvalitātes jomā, atvieglotu dalībvalstīm ES informācijas sistēmu tehnisko un operatīvo īstenošanu, pastiprinātu attiecīgajām ES informācijas sistēmām piemērojamos datu drošības un datu aizsardzības pasākumus, racionalizētu piekļuvi IIS, VIS, *ETIAS* un *Eurodac* nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus un atbalstītu IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

(11) Sadarbspējas komponentiem būtu jāaptver IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN*. Tiem būtu jāaptver arī Eiropola dati, bet vienīgi tiktāl, lai Eiropola datos varētu veikt vaicājumus vienlaikus ar minētajām ES informācijas sistēmām.

(12) Sadarbspējas komponentiem būtu jāapstrādā tādu personu personas dati, kuru personas dati tiek apstrādāti pamatā esošajās ES informācijas sistēmās un Eiropolā.

(13) Būtu jāizveido *ESP*, lai tehniski sekmētu dalībvalstu iestāžu un Savienības aģentūru ātru, netraucētu, efektīvu, sistemātisku un kontrolētu piekļuvi ES informācijas sistēmām, Eiropola datiem un Starptautiskās Kriminālpolicijas organizācijas (Interpola) datubāzēm, ciktāl tas vajadzīgs to uzdevumu izpildei un saskaņā ar to piekļuves tiesībām. *ESP* arī būtu jāatbalsta IIS, VIS, *ETIAS*, *Eurodac*, *SIS*, *ECRIS-TCN* un Eiropola datu mērķi. Nodrošinot iespēju paralēli veikt vaicājumus visās attiecīgajās ES informācijas sistēmās, kā arī Eiropola datos un Interpola datubāzēs, *ESP* būtu jādarbojas kā vienloga sistēmai jeb "ziņojumu starpniekam", lai meklētu datus dažādās centrālajās sistēmās un netraucēti izgūtu vajadzīgo informāciju, pilnībā ievērojot pamatā esošo sistēmu prasības attiecībā uz piekļuves kontroli un datu aizsardzību.

(14) *ESP* uzbūvei būtu jānodrošina, ka dati, ko *ESP* lietotājs izmanto vaicājuma veikšanai Interpola datubāzēs, netiek atklāti Interpola datu īpašniekiem. *ESP* uzbūvei būtu arī jānodrošina, lai vaicājumi Interpola datubāzē tiktu veikti vienīgi saskaņā ar piemērojamiem Savienības un valsts tiesību aktiem.

(15) Tiem *ESP* lietotājiem, kam ir tiesības piekļūt Eiropola datiem saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/794 ([4]), būtu jāvar veikt vaicājumu Eiropola datos vienlaikus ar ES informācijas sistēmām, kurām viņiem ir piekļuve. Jebkādai turpmākai pēc šāda vaicājuma veiktai datu apstrādei būtu jānotiek saskaņā ar Regulu (ES) 2016/794, tostarp attiecībā uz datu sniedzēja noteiktajiem piekļuves vai izmantošanas ierobežojumiem.

(16) *ESP* būtu jāizstrādā un jākonfigurē tā, lai tas ļautu veikt vaicājumus, vienīgi izmantojot datus, kas saistīti ar personām vai ceļošanas dokumentiem, kuri ir ietverti kādā ES informācijas sistēmā, Eiropola datos vai Interpola datubāzēs.

(17) Lai nodrošinātu attiecīgo ES informācijas sistēmu sistemātisku izmantošanu, *ESP* būtu jāizmanto, lai veiktu vaicājumus *CIR*, IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN*. Tomēr būtu jāsaglabā valsts pieslēgums dažādajām ES informācijas sistēmām, lai nodrošinātu tehnisku rezerves mehānismu. Arī Savienības aģentūrām būtu jāizmanto *ESP*, lai savu uzdevumu izpildes nolūkā veiktu vaicājumus centrālajā *SIS* saskaņā ar savām piekļuves tiesībām. *ESP* vajadzētu būt papildu līdzeklim, ar ko veikt vaicājumus centrālajā *SIS*, Eiropola datos un Interpola datubāzēs, papildinot esošās specializētās saskarnes.

(18) Biometriskie dati, piemēram, pirkstu nospiedumi un sejas attēli, ir unikāli un tādēļ personas identifikācijas mērķiem daudz ticamāki nekā burtciparu dati. Kopējam *BMS* vajadzētu būt tehniskam rīkam, kas pastiprina un atvieglo attiecīgo ES informācijas sistēmu un pārējo sadarbspējas komponentu darbu. Kopējā *BMS* galvenajam mērķim vajadzētu būt atvieglot vairākās datubāzēs reģistrētas personas identifikāciju, izmantojot vienu tehnoloģisko komponentu, lai salīdzinātu minētās personas biometriskos datus, kas atrodami dažādās sistēmās, tā vietā, lai izmantotu vairākus komponentus. Kopējam *BMS* būtu jāveicina drošība, kā arī jārada finansiāli, ar uzturēšanu saistīti un operatīvi ieguvumi. Visas automatizētās pirkstu nospiedumu identifikācijas sistēmas, tostarp tās, kas pašlaik tiek izmantotas *Eurodac*, VIS un *SIS*, izmanto biometriskās veidnes, kurās ir dati, kas iegūti faktisko biometrisko paraugu iezīmju izgūšanas rezultātā. Kopējam *BMS* būtu jāpārgrupē un jāglabā visas šīs biometriskās veidnes vienā vietā, tās loģiski nodalot pēc informācijas sistēmas, no kuras dati ir iegūti, tādējādi atvieglojot salīdzināšanu starp dažādām sistēmām ar biometriskajām veidnēm un ļaujot gūt apjomradītus ietaupījumus ES centrālo sistēmu izstrādē un uzturēšanā.

(19) Kopējā *BMS* glabātajām biometriskajām veidnēm būtu jāsastāv no datiem, kas atvasināti faktisko biometrisko paraugu iezīmju izgūšanas rezultātā un iegūti tādā veidā, ka šis izgūšanas process ir neatgriezenisks. Biometriskās veidnes būtu jāiegūst no biometriskajiem datiem, taču nevajadzētu būt iespējamam tos pašus biometriskos datus iegūt no biometriskajām veidnēm. Tā kā plaukstas nospiedumi un DNS profili tiek glabāti tikai *SIS*, izmantoti tikai *SIS* vajadzībām un tos nevar izmantot salīdzināšanai ar datiem citās informācijas sistēmās, ievērojot nepieciešamības un proporcionalitātes principus, kopējā *BMS* nebūtu jāglabā DNS profili vai biometriskās veidnes, kas iegūtas no plaukstas nospiedumu datiem.

(20) Biometriskie dati ir sensitīvi personas dati. Ar šo regulu būtu jānosaka pamats un drošības pasākumi šādu datu apstrādei nolūkā unikāli identificēt attiecīgās personas.

(21) IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN* nepieciešama precīza to personu identifikācija, kuru dati tajās tiek glabāti. Tāpēc *CIR* būtu jāatvieglo minētajās sistēmās reģistrēto personu pareiza identifikācija.

(22) Minētajās ES informācijas sistēmās glabātie personas dati var attiekties uz vienām un tām pašām personām, taču ar atšķirīgām vai nepilnīgām identitātēm. Dalībvalstu rīcībā ir efektīvi līdzekļi, kā savā teritorijā identificēt savus pilsoņus vai reģistrētos pastāvīgos iedzīvotājus. ES informācijas sistēmu sadarbspējai būtu jāpalīdz pareizi identificēt personas, kas tajās atrodamas. *CIR* būtu jāglabā personas dati, kas ir vajadzīgi, lai varētu precīzāk identificēt personas, kuru dati tiek glabāti minētajās sistēmās, tostarp viņu identitātes dati, ceļošanas dokumentu dati un biometriskie dati – neatkarīgi no tā, kurā sistēmā šie dati bija sākotnēji vākti. *CIR* būtu jāglabā tikai tie personas dati, kas ir noteikti vajadzīgi, lai veiktu precīzu identitātes pārbaudi. *CIR* reģistrētie personas dati būtu jāglabā ne ilgāk, kā tas ir noteikti nepieciešams pamatā esošo sistēmu nolūkos, un tie būtu automātiski jādzēš brīdī, kad datus dzēš pamatā esošajās sistēmās saskaņā ar šo datu loģisko nošķirumu.

([4]) 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.).

(23) Ir vajadzīga jauna apstrādes darbība, kas izpaužas kā šādu datu glabāšana *CIR*, nevis katrā atsevišķā sistēmā, lai būtu iespējams paaugstināt identifikācijas precizitāti, izmantojot datu automatizētu salīdzināšanu un atbilstību konstatēšanu. Tam, ka identitātes dati, ceļošanas dokumenta dati un biometriskie dati tiek glabāti *CIR*, nekādi nebūtu jākavē datu apstrāde IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN* nolūkos, jo *CIR* vajadzētu būt minēto pamatā esošo sistēmu jaunam kopīgam komponentam.

(24) Tāpēc nepieciešams *CIR* izveidot individuālu datni par katru personu, kura reģistrēta IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, lai sasniegtu mērķi Šengenas zonas iekšienē pareizi identificēt personas un atbalstīt *MID* nolūkā sasniegt divējādu mērķi, proti, atvieglot *bona fide* ceļotāju identitātes pārbaudes un apkarot identitātes viltošanu. Individuālajai datnei būtu jāglabā vienā vienīgā vietā visa ar personu saistītā identitātes informācija un jādara tā pieejama pienācīgi pilnvarotiem galalietotājiem.

(25) Tādējādi *CIR* būtu jāatvieglo un jāracionalizē par teroristu nodarījumu un citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu vai izmeklēšanu atbildīgo iestāžu piekļuve tādām ES informācijas sistēmām, kuras nav izveidotas tikai un vienīgi tam, lai novērstu, atklātu vai izmeklētu smagus noziegumus.

(26) Ar *CIR* būtu jāizveido kopīga personu, kuras reģistrētas IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN*, identitātes datu, ceļošanas dokumentu datu un biometrisko datu krātuve. Tam vajadzētu ietilpt minēto sistēmu tehniskajā arhitektūrā un darboties kā to kopīgam komponentam identitātes datu, ceļošanas dokumentu datu un biometrisko datu, kurus tās apstrādā, glabāšanai un vaicājumu veikšanai tajās.

(27) Visi *CIR* esošie ieraksti būtu loģiski jānodala, automātiski marķējot katru ierakstu ar tās pamatā esošās sistēmas nosaukumu, kurai pieder minētais ieraksts. Kontrolei attiecībā uz piekļuvi *CIR* būtu jāizmanto šie marķējumi, lai noteiktu, vai atļaut vai neatļaut piekļuvi attiecīgajam ierakstam.

(28) Ja dalībvalsts policijas iestāde nespēj identificēt personu, jo tai nav ceļošanas dokumenta vai cita ticama dokumenta, kas apliecinātu personas identitāti, vai ja pastāv šaubas par minētās personas sniegtajiem identitātes datiem vai par ceļošanas dokumenta autentiskumu, vai tā turētāja identitāti, vai ja attiecīgā persona nav spējīga vai atsakās sadarboties, šai policijas iestādei vajadzētu būt iespējai veikt vaicājumu *CIR*, lai identificētu attiecīgo personu. Šajā nolūkā policijas iestādēm pirkstu nospiedumi būtu jāiegūst ar tiešās skenēšanas pirkstu nospiedumu ņemšanas metodēm – ar noteikumu, ka procedūra tika sākta attiecīgās personas klātbūtnē. Šādi vaicājumi *CIR* nebūtu jāatļauj nolūkā identificēt nepilngadīgos, kas ir jaunāki par 12 gadiem, izņemot gadījumus, kad tas ir bērna interesēs.

(29) Ja personas biometriskie dati nav izmantojami vai ja vaicājums uz šo datu pamata nav rezultatīvs, vaicājums būtu jāveic, izmantojot minētās personas identitātes datus apvienojumā ar ceļošanas dokumenta datiem. Gadījumos, kad vaicājuma rezultātā noskaidrojas, ka dati par minēto personu tiek glabāti *CIR*, dalībvalstu iestādēm vajadzētu būt piekļuvei *CIR*, lai aplūkotu minētās personas identitātes datus un ceļošanas dokumenta datus, *CIR* nesniedzot nekādu norādi par to, kurai ES informācijas sistēmai šie dati pieder.

(30) Dalībvalstīm būtu jāpieņem valsts tiesību akti, ar kuriem nosaka iestādes, kas ir kompetentas veikt identitātes pārbaudes, izmantojot *CIR*, un nosakot šādu pārbaužu procedūras, nosacījumus un kritērijus, kam būtu jāievēro proporcionalitātes princips. Valsts tiesību aktos jo īpaši būtu jāparedz pilnvaras iegūt biometriskos datus tādas personas identitātes pārbaudes laikā, kura fiziski atrodas pie minēto iestāžu darbinieka.

(31) Ar šo regulu būtu arī jāievieš jauna iespēja, saskaņā ar kuru dalībvalsts izraudzītām iestādēm, kas ir atbildīgas par teroristu nodarījumu un smagu noziedzīgu nodarījumu novēršanu, atklāšanu vai izmeklēšanu, un Eiropolam ir racionalizēta piekļuve datiem, kas ietver ne tikai IIS, VIS, *ETIAS* vai *Eurodac* esošos identitātes vai ceļošanas dokumentu datus. Šādi dati var būt vajadzīgi, lai kādā konkrētā lietā novērstu, atklātu vai izmeklētu teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, ja ir pamatots iemesls uzskatīt, ka datu aplūkošana palīdzēs novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, jo īpaši, ja ir aizdomas, ka persona, ko tur aizdomās par teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu, šāda nodarījuma izdarītājs vai tajā cietušais ir persona, kuras dati tiek glabāti IIS, VIS, *ETIAS* vai *Eurodac*.

(32) Piemērojamiem tiesību instrumentiem arī turpmāk būtu jāreglamentē pilnīga piekļuve ES informācijas sistēmās esošajiem datiem, kuri vajadzīgi teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanai, atklāšanai vai izmeklēšanai un kuri nav tikai attiecīgie *CIR* ietvertie identitātes dati vai ceļošanas dokumentu dati. Izraudzītās iestādes, kas ir atbildīgas par teroristu nodarījumu un citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu vai izmeklēšanu, un Eiropols iepriekš nezina, kurā ES informācijas sistēmā ir to personu dati, attiecībā uz kurām tām jāveic vaicājums. Tas rada aizkavēšanos un neefektivitāti. Tāpēc izraudzītās iestādes pilnvarotajam galalietotājam būtu jāatļauj redzēt, kurā no minētajām ES informācijas sistēmām ir reģistrēti dati, kas iegūti vaicājuma rezultātā. Tādējādi pēc tam, kad būtu automatizēti verificēta atbilstības esamība sistēmā, attiecīgā sistēma tiktu apzīmēta ar karodziņu (tā dēvētā atbilstības karodziņu funkcija).

(33) Šajā kontekstā atbilde no *CIR* nav interpretējama vai izmantojama kā pamatojums vai iemesls izdarīt secinājumus par personu vai veikt pret to vērstus pasākumus, un tā būtu jāizmanto tikai, lai iesniegtu pieprasījumu piekļūt pamatā esošajām ES informācijas sistēmām, ievērojot nosacījumus un procedūras, kas paredzētas attiecīgajos tiesību aktos, kuri reglamentē šādu piekļuvi. Jebkuram šādam piekļuves pieprasījumam vajadzētu būt reglamentētam ar šīs regulas VII nodaļu un attiecīgi Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([5]), Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680 ([6]) vai Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 ([7]).

(34) Principā, ja atbilstības karodziņš rāda, ka dati ir reģistrēti *Eurodac*, izraudzītajām iestādēm vai Eiropolam būtu jāpieprasa pilnīga piekļuve vismaz vienai no attiecīgajām ES informācijas sistēmām. Ja izņēmuma gadījumā šāda pilnīga piekļuve netiek prasīta, jo, piemēram, izraudzītās iestādes vai Eiropols datus jau ir ieguvušas citādi vai valsts tiesību akti datu iegūšanu vairs neatļauj, būtu jāreģistrē piekļuves nepieprasīšanas pamatojums.

(35) Reģistra ierakstos par *CIR* veiktajiem vaicājumiem būtu jānorāda vaicājuma nolūks. Ja šāds vaicājums tika veikts, izmantojot divpakāpju pieeju datu aplūkošanai, reģistra ierakstos būtu jāiekļauj atsauce uz izmeklēšanas vai lietas valsts datni, tādējādi norādot, ka vaicājums tiks sākts teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, atklāšanas vai izmeklēšanas nolūkā.

(36) Lai izraudzītā iestāde un Eiropols varētu veikt vaicājumu *CIR* ar nolūku iegūt atbilstības karodziņa veida atbildi, kurā norādīts, ka dati ir reģistrēti IIS, VIS, *ETIAS* vai *Eurodac*, ir nepieciešama automatizēta personas datu apstrāde. Atbilstības karodziņam nebūtu jāatklāj attiecīgās personas personas dati, izņemot to, ka daļa no šīs personas datiem tiek glabāti vienā no sistēmām. Pilnvarotajam galalietotājam nebūtu jāpieņem nekādi nelabvēlīgi lēmumi attiecībā uz attiecīgo personu, pamatojoties vienīgi uz atbilstības karodziņa vienkāršu parādīšanos. Tādēļ piekļuve, kura piešķirta atbilstības karodziņa galalietotājam, radīs ļoti ierobežotu iejaukšanos attiecīgās personas tiesībās uz personas datu aizsardzību, vienlaikus atļaujot izraudzītajām iestādēm un Eiropolam efektīvāk pieprasīt piekļuvi personas datiem.

(37) Būtu jāizveido *MID*, lai sekmētu *CIR* darbību un atbalstītu IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus. Lai visas šīs ES informācijas sistēmas būtu efektīvas savu attiecīgo mērķu izpildē, tām ir nepieciešama precīza tādu personu identifikācija, kuru personas dati tajās tiek glabāti.

(38) Lai labāk sasniegtu ES informācijas sistēmu mērķus, iestādēm, kas izmanto šīs sistēmas, vajadzētu būt iespējai veikt pietiekami ticamas tādu personu identitātes verifikācijas, kuru dati tiek glabāti dažādās sistēmās. Konkrētajā atsevišķajā sistēmā glabāto identitātes vai ceļošanas dokumentu datu kopums var būt nepareizs, nepilnīgs vai

([5]) 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.).

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

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

maldinošs, un pašlaik nav iespējas konstatēt nepareizus, nepilnīgus vai maldinošus identitātes vai ceļošanas dokumentu datus, veicot salīdzināšanu ar citā sistēmā glabātiem datiem. Lai šo situāciju labotu, Savienības līmenī ir vajadzīgs tehnisks instruments, kas šajos nolūkos ļautu precīzi identificēt personas.

(39) Ar *MID* būtu jāizveido un jāglabā saiknes starp datiem dažādās ES informācijas sistēmās, lai konstatētu vairākas identitātes, nolūkā sasniegt divējādu mērķi, proti, atvieglot *bona fide* ceļotāju identitātes pārbaudes un apkarot identitātes viltošanu. *MID* būtu jāietver tikai saiknes starp datiem attiecībā uz personām, kuras atrodamas vairāk nekā vienā ES informācijas sistēmā. Saistītie dati būtu stingri jāierobežo, ietverot tikai tos, kas vajadzīgi, lai pārbaudītu, vai attiecīgā persona dažādās sistēmās pamatoti vai nepamatoti ir reģistrēta ar dažādām identitātēm, vai precizētu, ka divas personas ar līdzīgiem identitātes datiem var nebūt viena un tā pati persona. Datu apstrāde, ko veic, izmantojot *ESP* un kopējo *BMS*, lai saistītu individuālas personu datnes atsevišķu sistēmu starpā, būtu jānotur absolūta minimuma robežās, un tāpēc jāizmanto tikai vairāku identitāšu konstatēšanai, kas veicama, kad kāda no sistēmām, kuras dati tiek glabāti *CIR* vai pievienoti *SIS*, tiek papildināta ar jauniem datiem. *MID* būtu jāietver drošības pasākumi pret iespējamu diskrimināciju un nelabvēlīgiem lēmumiem attiecībā uz personām ar vairākām likumīgām identitātēm.

(40) Ar šo regulu tiek noteiktas jaunas datu apstrādes darbības, kuru mērķis ir pareizi identificēt attiecīgās personas. Tā ir iejaukšanās viņu pamattiesībās, kas tiek aizsargātas ar Eiropas Savienības Pamattiesību hartas 7. un 8. pantu. Tā kā efektīva ES informācijas sistēmu īstenošana ir atkarīga no pareizas attiecīgo personu identifikācijas, šāda iejaukšanās ir pamatota ar tiem pašiem mērķiem, kuru dēļ katra no šīm sistēmām ir izveidota, proti, ar efektīvu Savienības robežu pārvaldību, Savienības iekšējo drošību un Savienības patvēruma un vīzu politikas efektīvu īstenošanu.

(41) *ESP* un kopējam *BMS* būtu jāsalīdzina *CIR* un *SIS* esošie dati par personām tad, kad valsts iestāde vai Savienības aģentūra izveido vai augšupielādē jaunus ierakstus. Šādai salīdzināšanai vajadzētu būt automatizētai. *CIR* un *SIS* būtu jāizmanto kopējais *BMS*, lai atklātu iespējamas saiknes, kuru pamatā ir biometriskie dati. *CIR* un *SIS* būtu jāizmanto *ESP*, lai atklātu iespējamas saiknes, kuru pamatā ir burtciparu dati. *CIR* un *SIS* būtu jāvar identificēt vairākās sistēmās glabātus tādus pašus vai līdzīgus datus par personu. Tādā gadījumā būtu jāizveido saikne, kas norāda, ka tā ir viena un tā pati persona. *CIR* un *SIS* būtu jākonfigurē tā, lai nelielas transliterācijas vai pareizrakstības kļūdas tiktu atklātas tādā veidā, kas attiecīgajai personai neradītu nekādus nepamatotus šķēršļus.

(42) Valsts iestādei vai Savienības aģentūrai, kas reģistrēja datus attiecīgajā ES informācijas sistēmā, būtu jāapstiprina vai jāmaina šīs saiknes. Šai valsts iestādei vai Savienības aģentūrai atšķirīgu identitāšu manuālas verifikācijas nolūkā vajadzētu būt piekļuvei datiem, kas tiek glabāti *CIR* vai *SIS* un *MID*.

(43) Atšķirīgu identitāšu manuāla verifikācija būtu jāveic iestādei, kura izveidoja vai atjauninjust datus, kas izraisīja atbilstības rādījumu, kura rezultātā tika izveidota saikne ar citā ES informācijas sistēmā jau glabātajiem datiem. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai iestādei būtu jānovērtē, vai pastāv vairākas identitātes, kas pamatoti vai nepamatoti attiecas uz vienu un to pašu personu. Šāds novērtējums iespēju robežās būtu jāveic attiecīgās personas klātbūtnē, vajadzības gadījumā pieprasot papildu paskaidrojumus vai informāciju. Novērtējums būtu jāveic nekavējoties un saskaņā ar juridiskajām prasībām par informācijas precizitāti, ko paredz Savienības un valsts tiesību akti.

(44) Tādu saikņu gadījumā, kuras iegūtas *SIS* ietvaros un saistītas ar brīdinājumiem par personām, ko meklē, lai apcietinātu nolūkā tās nodot vai izdot, par pazudušām personām vai neaizsargātām personām, par personām, ko cenšas atrast, lai tās varētu palīdzēt tiesas procesā, vai par personām diskrētu pārbaužu, izmeklēšanas pārbaužu vai īpašu pārbaužu vajadzībām, par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai iestādei vajadzētu būt tās dalībvalsts *SIRENE* birojam, kura izveidoja brīdinājumu. Minēto kategoriju *SIS* brīdinājumi ir sensitīvi un nebūtu

obligāti jāizpauž iestādēm, kas izveido vai atjaunina ar tiem saistītos datus vienā no pārējām ES informācijas sistēmām. Saiknes ar *SIS* datiem izveidei nebūtu jāskar darbības, kas ir jāveic saskaņā ar Eiropas Parlamenta un Padomes Regulām (ES) 2018/1860 ([8]), (ES) 2018/1861 ([9]) un (ES) 2018/1862 ([10]).

(45) Šādu saikņu izveidē ir vajadzīga pārredzamība attiecībā pret to skartajām personām. Lai atvieglotu nepieciešamo drošības pasākumu īstenošanu saskaņā ar piemērojamiem Savienības datu aizsardzības noteikumiem, personas, par kurām pēc atšķirīgu identitāšu manuālas verifikācijas ir izveidota sarkana vai balta saikne, būtu rakstiski jāinformē, neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību vai sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta valsts veikta izmeklēšana. Minētajām personām būtu jāsaņem vienots identifikācijas numurs, kas dotu iespēju identificēt iestādi, kurā tām jāvēršas, lai izmantotu savas tiesības.

(46) Ja ir izveidota dzeltena saikne, iestādei, kura ir atbildīga par atšķirīgu identitāšu manuālu verifikāciju, vajadzētu būt piekļuvei *MID*. Ja pastāv sarkana saikne, dalībvalstu iestādēm un Savienības aģentūrām, kurām ir piekļuve vismaz vienai *CIR* iekļautajai ES informācijas sistēmai vai *SIS*, vajadzētu būt piekļuvei *MID*. Sarkanajai saiknei būtu jānorāda, ka persona nepamatoti izmanto atšķirīgas identitātes vai ka persona izmanto svešu identitāti.

(47) Ja pastāv balta vai zaļa saikne starp divu ES informācijas sistēmu datiem, dalībvalstu iestādēm un Savienības aģentūrām vajadzētu būt piekļuvei *MID*, ja šādai attiecīgajai iestādei vai aģentūrai ir piekļuve abām informācijas sistēmām. Šāda piekļuve būtu jāpiešķir tikai un vienīgi nolūkā ļaut minētajai iestādei vai aģentūrai atklāt potenciālus gadījumus, kad dati ir saistīti nepareizi vai tie apstrādāti *MID*, *CIR* un *SIS*, pārkāpjot šo regulu, un veikt darbības, lai labotu situāciju un atjauninātu vai dzēstu saikni.

(48) Eiropas Savienības Aģentūrai lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) būtu jāievieš automatizēti datu kvalitātes kontroles mehānismi un kopēji datu kvalitātes indikatori. *eu-LISA* vajadzētu būt pienākumam attīstīt centrālu spēju datu kvalitātes pārraudzībai un sagatavot regulārus datu analīzes ziņojumus nolūkā uzlabot kontroli pār to, kā dalībvalstis īsteno ES informācijas sistēmas. Kopējiem datu kvalitātes indikatoriem būtu jāietver minimālie kvalitātes standarti attiecībā uz datu glabāšanu ES informācijas sistēmās vai sadarbspējas komponentos. Šādu datu kvalitātes standartu mērķim vajadzētu būt panākt, ka ES informācijas sistēmas un sadarbspējas komponenti var automātiski identificēt acīmredzami kļūdainus vai nekonsekventus ievadītos datus, kā rezultātā izcelsmes dalībvalsts varētu verificēt šos datus un veikt visas vajadzīgās korektīvās darbības.

(49) Komisijai būtu jāizvērtē *eu-LISA* kvalitātes ziņojumi un vajadzības gadījumā jāsniedz ieteikumi dalībvalstīm. Dalībvalstīm vajadzētu būt pienākumam sagatavot rīcības plānu, kurā aprakstītas darbības visu ar datu kvalitāti saistīto trūkumu novēršanai, un būtu regulāri jāziņo par progresu šā rīcības plāna īstenošanā.

(50) Vienotajam ziņojuma formātam (*UMF*) būtu jākalpo kā standartam strukturētai pārrobežu informācijas apmaiņai starp informācijas sistēmām, iestādēm vai organizācijām tieslietu un iekšlietu jomā. *UMF* būtu jānosaka kopēja terminoloģija un loģiskās struktūras attiecībā uz kopīgi apmainītu informāciju, lai atvieglotu sadarbspēju, ļaujot saskaņotā un semantiski līdzvērtīgā veidā izveidot un lasīt apmainītās informācijas saturu.

(51) Var apsvērt iespēju *UMF* standartu izmantot VIS, *SIS* un jebkuros citos esošajos vai jaunajos pārrobežu informācijas apmaiņas modeļos un informācijas sistēmās, ko dalībvalstis izstrādājušas tieslietu un iekšlietu jomā.

([8]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1860 (2018. gada 28. novembris) par Šengenas informācijas sistēmas izmantošanu to trešo valstu valstspiederīgo atgriešanai, kuri dalībvalstīs uzturas nelikumīgi (OV L 312, 7.12.2018., 1. lpp.).

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1861 (2018. gada 28. novembris) 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 312, 7.12.2018., 14. lpp.).

([10]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1862 (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 (OV L 312, 7.12.2018., 56. lpp.).

(52) Būtu jāizveido centrāls ziņošanas un statistikas repozitorijs (*CRRS*), lai politikas, operatīvos un datu kvalitātes nolūkos saskaņā ar piemērojamajiem tiesību instrumentiem iegūtu vairākas sistēmas aptverošus statistikas datus un analītiskus ziņojumus. *eu-LISA* būtu jāizveido, jāīsteno un jāmitina *CRRS* savos tehniskajos centros. Tajā būtu jāietver anonimizēti statistikas dati no ES informācijas sistēmām, *CIR*, *MID* un kopējā *BMS*. *CRRS* ietvertajiem datiem nebūtu jādod iespēja identificēt atsevišķas personas. *eu-LISA* būtu automatizēti jāpadara dati anonīmi un jāreģistrē šādi anonimizēti dati *CRRS*. Datu anonimizācijas procesam vajadzētu būt automatizētam, un *eu-LISA* darbiniekiem nebūtu jāpiešķir tieša piekļuve ES informācijas sistēmās vai sadarbspējas komponentos glabātiem personas datiem.

(53) Personas datu apstrādei sadarbspējas nolūkā, ko valstu iestādes veic saskaņā ar šo regulu, piemēro Regulu (ES) 2016/679, ja vien šādu apstrādi dalībvalstu izraudzītās iestādes vai centrālie piekļuves punkti neveic teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, atklāšanas vai izmeklēšanas nolūkos.

(54) Ja dalībvalstu veiktu personas datu apstrādi atbilstīgi šai regulai sadarbspējas nolūkā veic kompetentās iestādes teroristu nodarījumu vai citu smagu noziedzīgu nodarījumu novēršanas, atklāšanas vai izmeklēšanas nolūkos, piemēro Direktīvu (ES) 2016/680.

(55) Jebkādu personas datu nosūtīšanai uz trešām valstīm vai starptautiskajām organizācijām, ko veic atbilstīgi šai regulai, piemēro arī Regulu (ES) 2016/679, Regulu (ES) 2018/1725 vai attiecīgos gadījumos Direktīvu (ES) 2016/680. Neskarot Regulas (ES) 2016/679 V nodaļā vai attiecīgā gadījumā Direktīvā (ES) 2016/680 paredzētos nosūtīšanas pamatus, ikviens trešās valsts tiesas spriedums un ikviens trešās valsts administratīvās iestādes lēmums, kurā pārzinim vai apstrādātājam pieprasīts nosūtīt vai izpaust personas datus, būtu jāatzīst vai jāizpilda vienīgi tad, ja tas ir balstīts uz starptautisku nolīgumu, kas ir spēkā starp pieprasītāju trešo valsti un Savienību vai kādu tās dalībvalsti.

(56) Īpašos datu aizsardzības noteikumus, kas paredzēti Regulā (ES) 2018/1862 un Eiropas Parlamenta un Padomes Regulā (ES) 2019/816 ([11]), piemēro personas datu apstrādei ar minētajām regulām reglamentētajās sistēmās.

(57) Personas datu apstrādei, ko *eu-LISA* un citas Savienības iestādes un struktūras veic, pildot savus pienākumus saskaņā ar šo regulu, piemēro Regulu (ES) 2018/1725, neskarot Regulu (ES) 2016/794, kuru piemēro personas datu apstrādei, ko veic Eiropols.

(58) Dalībvalstu veiktās personas datu apstrādes likumība būtu jāuzrauga uzraudzības iestādēm, kas minētas Regulā (ES) 2016/679 vai Direktīvā (ES) 2016/680. Eiropas Datu aizsardzības uzraudzītājam būtu jāuzrauga Savienības iestāžu un struktūru darbības, kas saistītas ar personas datu apstrādi. Eiropas Datu aizsardzības uzraudzītājam un uzraudzības iestādēm, uzraugot personas datu apstrādi, ko veic ar sadarbspējas komponentu palīdzību, būtu savstarpēji jāsadarbojas. Lai Eiropas Datu aizsardzības uzraudzītājs varētu pildīt tam ar šo regulu uzticētos uzdevumus, ir vajadzīgi pietiekami papildu resursi, tostarp gan cilvēkresursi, gan finansiālie resursi.

(59) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001 ([12]) 28. panta 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2018. gada 16. aprīlī ([13]) ir sniedzis atzinumu.

(60) 29. panta datu aizsardzības darba grupa 2018. gada 11. aprīlī sniedza atzinumu.

(61) Gan dalībvalstīm, gan *eu-LISA* būtu jāuztur drošības plāns, lai atvieglotu drošības saistību izpildi, un tām būtu jāsadarbojas, lai risinātu drošības jautājumus. *eu-LISA* būtu arī jāgādā par to, ka pastāvīgi tiek izmantoti jaunākie tehnoloģiskie sasniegumi, lai nodrošinātu datu integritāti saistībā ar sadarbspējas komponentu izstrādi, projektēšanu un pārvaldību. Šajā ziņā *eu-LISA* pienākumos vajadzētu būt arī pieņemt pasākumus, kas vajadzīgi,

([11]) Eiropas Parlamenta un Padomes 2019. gada Regula (ES) 2019/816 (2019. gada 17. aprīlis), ar ko Eiropas Sodāmības reģistru informācijas sistēmas papildināšanai un atbalstam izveido centralizētu sistēmu (*ECRIS-TCN*) tādu dalībvalstu identificēšanai, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un ar ko groza Regulu (ES) 2018/1726 (skatīt šā *Oficiālā Vēstneša* 1. lpp.).

([12]) 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.).

([13]) OV C 233, 4.7.2018., 12. lpp.

lai liegtu nepilnvarotu personu, piemēram, ārpakalpojumu sniedzēju darbinieku, piekļuvi personas datiem, kuri tiek apstrādāti ar sadarbspējas komponentiem. Piešķirot tiesības slēgt pakalpojumu līgumus, dalībvalstīm un *eu-LISA* būtu jāapsver visi pasākumi, kas vajadzīgi, lai nodrošinātu atbilstību tiesību aktiem vai noteikumiem, kuri saistīti ar personas datu un privātuma aizsardzību, vai sargātu būtiskas drošības intereses, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2018/1046 ([14]) un piemērojamās starptautiskās konvencijas. *eu-LISA* sadarbspējas komponentu izstrādes gaitā būtu jāievēro integrētas privātuma aizsardzības un privātuma aizsardzības pēc noklusējuma principi.

(62) Lai sekmētu statistikas un ziņošanas mērķus, ir jāpiešķir piekļuve šajā regulā minēto kompetento iestāžu, Savienības iestāžu un aģentūru pilnvarotiem darbiniekiem, lai viņi varētu aplūkot konkrētus ar konkrētiem sadarbspējas komponentiem saistītus datus, nedodot viņiem iespēju identificēt personas.

(63) Lai ļautu dalībvalstu iestādēm un Savienības aģentūrām pielāgoties jaunajām prasībām par *ESP* izmantošanu, ir jāparedz pārejas periods. Līdzīgi, lai nodrošinātu *MID* saskaņotu un optimālu darbību, būtu jānosaka pārejas pasākumi attiecībā uz tā darbības sākumu.

(64) Ņemot vērā to, ka šīs regulas mērķi, proti, izveidot ES informācijas sistēmu sadarbspējas satvaru, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet šīs rīcības mēroga un iedarbības dēļ to 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 minētā mērķa sasniegšanai.

(65) Atlikusī summa budžetā, kurš ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 515/2014 ([15]) ir piešķirts viedrobežām, būtu jāpārdala šai regulai saskaņā ar Regulas (ES) Nr. 515/2014 5. panta 5. punkta b) apakšpunktu, lai segtu sadarbspējas komponentu izstrādes izmaksas.

(66) Lai papildinātu konkrētus detalizētus šīs regulas tehniskos aspektus, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 290. pantu attiecībā uz:

— pārejas laikposma pagarināšanu *ESP* izmantošanai,

— pārejas laikposma pagarināšanu *ETIAS* centrālās vienības veiktai vairāku identitāšu konstatēšanai,

— procedūrām tādu gadījumu noteikšanai, kad identitāti var uzskatīt par tādu pašu vai līdzīgu,

— noteikumiem par *CRRS* darbību, tostarp īpašiem personas datu apstrādes aizsardzības pasākumiem un drošības noteikumiem, ko piemēro repozitorijam, un

— detalizētiem noteikumiem par tīmekļa portāla darbību.

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 ([16]). 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.

(67) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai, lai tā varētu noteikt datumus, kuros *ESP*, kopējam *BMS*, *CIR*, *MID* un *CRRS* jāsāk darboties.

([14]) Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2018/1046 (2018. gada 18. jūlijs) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam, ar kuru groza Regulas (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 un Lēmumu Nr. 541/2014/ES un atceļ Regulu (ES, Euratom) Nr. 966/2012 (OV L 193, 30.7.2018., 1. lpp.).

([15]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 515/2014 (2014. gada 16. aprīlis), ar ko kā daļu no Iekšējās drošības fonda izveido finansiāla atbalsta instrumentu ārējām robežām un vīzām un atceļ Lēmumu Nr. 574/2007/EK (OV L 150, 20.5.2014., 143. lpp.).

([16]) OV L 123, 12.5.2016., 1. lpp.

(68) Komisijai būtu arī jāpiešķir īstenošanas pilnvaras attiecībā uz sīki izstrādātu noteikumu pieņemšanu par: *ESP* lietotāju profilu tehniskajiem parametriem; specifikācijām tehniskajam risinājumam, kas ļauj, izmantojot *ESP*, veikt vaicājumus ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs, un *ESP* atbilžu formātu; tehniskajiem noteikumiem, kā *MID* izveidot saiknes starp datiem no dažādām ES informācijas sistēmām; tādas veidlapas saturu un izklāstu, ko izmanto, lai informētu datu subjektu sarkanas saiknes izveidošanas gadījumā; kopējā *BMS* snieguma prasībām un snieguma uzraudzību; automatizētiem datu kvalitātes kontroles mehānismiem, procedūrām un rādītājiem; *UMF* standarta izstrādi; sadarbības procedūru drošības incidenta gadījumā; tehniskā risinājuma specifikācijām, kurš paredzēts dalībvalstīm lietotāju piekļuves pieprasījumu pārvaldībai. Minētās pilnvaras būtu jāīsteno saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 ([17]).

(69) Tā kā sadarbspējas komponenti ietvers ievērojama sensitīvu personas datu daudzuma apstrādi, ir svarīgi, lai personas, kuru dati tiek apstrādāti, izmantojot minētos komponentus, var efektīvi īstenot savas datu subjektu tiesības, kā tas prasīts Regulā (ES) 2016/679, Direktīvā (ES) 2016/680 un Regulā (ES) 2018/1725. Datu subjektu vajadzībām būtu jānodrošina tīmekļa portāls, kas atvieglo viņiem īstenot savas tiesības piekļūt saviem personas datiem un tiesības uz personas datu labošanu, dzēšanu un apstrādes ierobežošanu. Šāds tīmekļa portāls būtu jāizveido un jāpārvalda *eu-LISA*.

(70) Viens no datu aizsardzības pamatprincipiem ir datu minimizēšana: atbilstīgi Regulas (ES) 2016/679 5. panta 1. punkta c) apakšpunktam personas datu apstrādei ir jābūt adekvātai, atbilstīgai un jāietver tikai tas, kas nepieciešams to apstrādes nolūkos. Tāpēc sadarbspējas komponentiem nebūtu jāparedz nekādu jaunu personas datu glabāšana, izņemot saiknes, kas tiks glabātas *MID* un kas ir šīs regulas nolūkiem vajadzīgais minimums.

(71) Šajā regulā būtu jāietver skaidri noteikumi par atbildību un tiesībām uz kompensāciju personas datu nelikumīgas apstrādes un jebkādas citas ar šo regulu nesaderīgas darbības gadījumā. Šādiem noteikumiem nebūtu jāskar tiesības uz kompensāciju no pārziņa vai apstrādātāja un pārziņa vai apstrādātāja atbildību saskaņā ar Regulu (ES) 2016/679, Direktīvu (ES) 2016/680 un Regulu (ES) 2018/1725. *eu-LISA*, kad tā darbojas kā datu apstrādātājs, vajadzētu būt atbildīgai par jebkādu kaitējumu, ko tā izraisījusi gadījumā, ja tā nav izpildījusi konkrētos šīs regulas pienākumus, kas tai noteikti, vai rīkojusies ārpus vai pretēji tās dalībvalsts likumīgiem norādījumiem, kura ir datu pārzinis.

(72) Šī regula neskar Eiropas Parlamenta un Padomes Direktīvas 2004/38/EK ([18]) piemērošanu.

(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, ciktāl tās noteikumi attiecas uz *SIS*, ko reglamentē Regula (ES) 2018/1862, papildina Šengenas *acquis*, Dānija saskaņā ar minētā protokola 4. pantu sešos mēnešos pēc tam, kad Padome pieņēmusi lēmumu par šo regulu, izlemj, vai tā šo regulu ieviesīs savos tiesību aktos.

(74) Ciktāl šīs regulas noteikumi attiecas uz *SIS*, ko reglamentē Regula (ES) 2018/1862, Apvienotā Karaliste piedalās šajā regulā saskaņā ar 5. panta 1. punktu Protokolā Nr. 19 par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā, kurš pievienots LES un LESD, un 8. panta 2. punktu Lēmumā 2000/365/EK ([19]). Turklāt, ciktāl šīs regulas noteikumi attiecas uz *Eurodac* un *ECRIS-TCN*, saskaņā ar 3. pantu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots LES un LESD, Apvienotā Karaliste ar 2018. gada 18. maija vēstuli ir paziņojusi savu vēlmi piedalīties šīs regulas pieņemšanā un piemērošanā.

([17]) 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.).

([18]) Eiropas Parlamenta un Padomes Direktīva 2004/38/EK (2004. gada 29. aprīlis) par Savienības pilsoņu un viņu ģimenes locekļu tiesībām brīvi pārvietoties un dzīvot dalībvalstu teritorijā, ar ko groza Regulu (EEK) Nr. 1612/68 un atceļ Direktīvas 64/221/EEK, 68/360/EEK, 72/194/EEK, 73/148/EEK, 75/34/EEK, 75/35/EEK, 90/364/EEK, 90/365/EEK un 93/96/EEK (OV L 158, 30.4.2004., 77. lpp.).

([19]) 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) Ciktāl šīs regulas noteikumi attiecas uz *SIS*, ko reglamentē Regula (ES) 2018/1862, Īrija principā varētu piedalīties šajā regulā saskaņā ar 5. panta 1. punktu Protokolā Nr. 19 par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā, kurš pievienots LES un LESD, un 6. panta 2. punktu Padomes Lēmumā 2002/192/EK ([20]) Turklāt, ciktāl šīs regulas noteikumi attiecas uz *Eurodac* un *ECRIS-TCN*, saskaņā ar 1. un 2. pantu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots LES un LESD, un neskarot 4. pantu minētajā protokolā, Īrija nepiedalās šīs regulas pieņemšanā un tai šī regula nav saistoša un nav jāpiemēro. Tā kā šādos apstākļos nav iespējams nodrošināt, ka šī regula visā tās kopumā ir piemērojama Īrijai, kā prasīts LESD 288. pantā, Īrija nepiedalās šīs regulas pieņemšanā un tai šī regula nav saistoša un nav jāpiemēro, neskarot tās tiesības, kas paredzētas Protokolos Nr. 19 un Nr. 21.

(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 ([21]), šī regula, ciktāl tā attiecas uz *SIS*, ko reglamentē Regula (ES) 2018/1862, ir to Šengenas *acquis* noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta 1. panta G punktā Padomes Lēmumā 1999/437/EK ([22]).

(77) Attiecībā uz Šveici – saskaņā ar Nolīgumu, kas noslēgts starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā ([23]), šī regula, ciktāl tā attiecas uz *SIS*, ko reglamentē Regula (ES) 2018/1862, ir to Šengenas *acquis* noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta Lēmuma 1999/437/EK 1. panta G punktā, kurus lasa saistībā ar Padomes Lēmuma 2008/149/TI ([24]) 3. pantu.

(78) Attiecībā uz Lihtenšteinu – saskaņā ar 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 ([25]), šī regula, ciktāl tā attiecas uz *SIS*, ko reglamentē Regula (ES) 2018/1862, ir to Šengenas *acquis* noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta Lēmuma 1999/437/EK 1. panta G punktā, kurus lasa saistībā ar Padomes Lēmuma 2011/350/ES ([26]) 3. pantu.

(79) Šī regula atbilst jo īpaši Eiropas Savienības Pamattiesību hartā atzītajām pamattiesībām un principiem un būtu jāpiemēro saskaņā ar minētajām tiesībām un principiem.

(80) Lai šo regulu ietvertu spēkā esošajā tiesiskajā regulējumā, būtu attiecīgi jāgroza Eiropas Parlamenta un Padomes Regula (ES) 2018/1726 ([27]) un Regulas (ES) 2018/1862 un (ES) 2019/816,

---

([20]) 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.).

([21]) OV L 176, 10.7.1999., 36. lpp.

([22]) 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.).

([23]) OV L 53, 27.2.2008., 52. lpp.

([24]) Padomes Lēmums 2008/149/TI (2008. gada 28. janvāris) par to, lai Eiropas Kopienas 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.).

([25]) OV L 160, 18.6.2011., 21. lpp.

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

([27]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1726 (2018. gada 14. novembris) 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 295, 21.11.2018., 99. lpp.).

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

Vispārīgi noteikumi

1. pants

Priekšmets

1. Ar šo regulu – kopā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/817 ([28]) – izveido satvaru sadarbspējas nodrošināšanai starp ieceļošanas/izceļošanas sistēmu (IIS), vīzu informācijas sistēmu (VIS), Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*), *Eurodac*, Šengenas Informācijas sistēmu (*SIS*) un Eiropas Sodāmības reģistru informācijas sistēmu trešo valstu valstspiederīgajiem (*ECRIS-TCN*).

2. Satvars ietver šādus sadarbspējas komponentus:

a) Eiropas meklēšanas portāls (*ESP*);

b) kopējs biometrisko datu salīdzināšanas pakalpojums (kopējais *BMS*);

c) kopējs identitātes repozitorijs (*CIR*);

d) vairāku identitāšu detektors (*MID*).

3. Šajā regulā ir arī paredzēti noteikumi par datu kvalitātes prasībām, vienotu ziņojuma formātu (*UMF*) un centrālu ziņošanas un statistikas repozitoriju (*CRRS*) un ir noteikti dalībvalstu un Eiropas Aģentūras lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) pienākumi attiecībā uz sadarbspējas komponentu uzbūvi, izstrādi un darbību.

4. Ar šo regulu arī pielāgo procedūras un nosacījumus, ko piemēro dalībvalstu izraudzīto iestāžu un Eiropas Savienības Aģentūras tiesībaizsardzības sadarbībai (Eiropola) piekļuvei IIS, VIS, *ETIAS* un *Eurodac* ar mērķi novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus.

5. Šī regula paredz arī satvaru personu identitātes verificēšanai un personu identificēšanai.

2. pants

Mērķi

1. Nodrošinot sadarbspēju, šai regulai ir šādi mērķi:

a) uzlabot robežpārbaužu iedarbīgumu un efektivitāti uz ārējām robežām;

b) sekmēt nelikumīgas imigrācijas novēršanu un apkarošanu;

c) sekmēt augsta drošības līmeņa panākšanu Savienības brīvības, drošības un tiesiskuma telpā, tostarp sabiedriskās drošības un sabiedriskās kārtības uzturēšanu un drošības saglabāšanu dalībvalstu teritorijās;

d) uzlabot kopējās vīzu politikas īstenošanu;

e) palīdzēt starptautiskās aizsardzības pieteikumu izskatīšanā;

f) palīdzēt novērst, atklāt un izmeklēt teroristu nodarījumus un citus smagus noziedzīgus nodarījumus;

g) palīdzēt identificēt nezināmas personas, kuras sevi identificēt nespēj, vai neidentificētas cilvēku mirstīgās atliekas dabas katastrofas, nelaimes gadījuma vai teroristu uzbrukuma gadījumā.

2. Šā panta 1. punkta minētos mērķus sasniedz:

a) nodrošinot personu pareizu identifikāciju;

b) palīdzot apkarot identitātes viltošanu;

([28]) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (skatīt šā *Oficiālā Vēstneša* 27. lpp.).

c) uzlabojot datu kvalitāti un saskaņojot prasības par ES informācijas sistēmās glabāto datu kvalitāti, vienlaikus ievērojot datu apstrādes prasības, kas noteiktas tiesību instrumentos, kuri reglamentē atsevišķās sistēmas, kā arī datu aizsardzības standartus un principus;

d) atvieglojot un atbalstot esošo ES informācijas sistēmu tehnisko un operatīvo īstenošanu dalībvalstīs;

e) pastiprinot, vienkāršojot un padarot saskaņotākus datu drošības un datu aizsardzības nosacījumus, kuri reglamentē attiecīgās ES informācijas sistēmas, taču neietekmējot īpašo aizsardzību un aizsardzības pasākumus, kas ir paredzēti konkrētām datu kategorijām;

f) racionalizējot nosacījumus par izraudzīto iestāžu piekļuvi IIS, VIS, *ETIAS* un *Eurodac* sistēmām, vienlaikus nodrošinot nepieciešamus un samērīgus minētās piekļuves nosacījumus;

g) atbalstot IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

3. pants

Darbības joma

1. Šo regulu piemēro *Eurodac*, *SIS* un *ECRIS-TCN*.

2. Šo regulu piemēro arī Eiropola datiem tiktāl, ka tiek radīta iespēja veikt tajos vaicājumus vienlaikus ar 1. punktā minētajām ES informācijas sistēmām.

3. Šo regulu piemēro personām, attiecībā uz kurām personas datus var apstrādāt 1. punktā minētajās ES informācijas sistēmās un 2. punktā minētajos Eiropola datos.

4. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "ārējās robežas" ir ārējās robežas, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2016/399 ([29]) 2. panta 2) punktā;

2) "robežpārbaudes" ir robežpārbaudes, kā definēts Regulas (ES) 2016/399 2. panta 11) punktā;

3) "robežu iestāde" ir robežsardze, kurai saskaņā ar valsts tiesību aktiem ir uzdots veikt robežpārbaudes;

4) "uzraudzības iestādes" ir uzraudzības iestāde, kas minēta Regulas (ES) 2016/679 51. panta 1. punktā, un uzraudzības iestāde, kas minēta Direktīvas (ES) 2016/680 41. panta 1. punktā;

5) "verifikācija" ir datu kopumu salīdzināšana nolūkā apstiprināt uzdotu identitāti (pārbaude "viens pret vienu");

6) "identifikācija" ir personas identitātes noteikšana, meklējot datubāzē un salīdzinot ar daudziem datu kopumiem (pārbaude "viens pret daudziem");

7) "burtciparu dati" ir dati, ko veido burti, cipari, īpašas zīmes, atstarpes un pieturzīmes;

8) "identitātes dati" ir dati, kas minēti 27. panta 3. punkta a)–e) apakšpunktā;

9) "pirkstu nospiedumu dati" ir pirkstu nospiedumu attēli un latentu pirkstu nospiedumu attēli, kuri, ņemot vērā to unikālās īpašības un tajos ietvertās atsauces vērtības, dara iespējamu precīzu un pārliecinošu salīdzināšanu attiecībā uz personas identitāti;

([29]) 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.).

10) "sejas attēls" ir digitāls personas sejas attēls;

11) "biometriskie dati" ir pirkstu nospiedumu dati vai sejas attēli, vai abi;

12) "biometriskā veidne" ir matemātisks attēlojums, kas iegūts no biometriskajiem datiem iezīmju izguves rezultātā un aprobežojas ar pazīmēm, kuras ir vajadzīgas identifikācijas un verifikācijas veikšanai;

13) "ceļošanas dokuments" ir pase vai cits līdzvērtīgs dokuments, kas tā turētājam dod tiesības šķērsot ārējās robežas un kam var piestiprināt vīzu;

14) "ceļošanas dokumenta dati" ir ceļošanas dokumenta veids, numurs un tā izdevēja valsts, ceļošanas dokumenta derīguma beigu termiņš un ceļošanas dokumenta izdevējas valsts trīs burtu kods;

15) "ES informācijas sistēmas" ir IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN*;

16) "Eiropola dati" ir personas dati, ko Eiropols apstrādājis Regulas (ES) 2016/794 18. panta 2. punkta a), b) un c) apakšpunktā minētajos nolūkos;

17) "Interpola datubāzes" ir Interpola Zagto un pazaudēto ceļošanas dokumentu (SLTD datubāze) datubāze un Interpola datubāze ar ceļošanas dokumentiem, par kuriem izdoti paziņojumi (*TDAWN* datubāze);

18) "atbilstība" ir atbilsme, kas ir konstatēta, automātiski salīdzinot personas datus, kuri ir reģistrēti vai tiek reģistrēti kādā informācijas sistēmā vai datubāzē;

19) "policijas iestāde" ir "kompetentā iestāde", kā definēts Direktīvas (ES) 2016/680 3. panta 7) punktā;

20) "izraudzītās iestādes" ir dalībvalstu izraudzītās iestādes, kas definētas Eiropas Parlamenta un Padomes Regulas (ES) 2017/2226 ([30]) 3. panta 1. punkta 26) apakšpunktā, Padomes Lēmuma 2008/633/TI ([31]) 2. panta 1. punkta e) apakšpunktā un Eiropas Parlamenta un Padomes Regulas (ES) 2018/1240 ([32]) 3. panta 1. punkta 21) apakšpunktā;

21) "teroristu nodarījums" ir valsts tiesību aktos minēts nodarījums, kas atbilst vai ir līdzvērtīgs vienam no nodarījumiem, kuri minēti Eiropas Parlamenta un Padomes Direktīvā (ES) 2017/541 ([33]);

22) "smags noziedzīgs nodarījums" ir nodarījums, kas atbilst vai ir līdzvērtīgs vienam no nodarījumiem, kuri minēti Padomes Pamatlēmuma 2002/584/TI ([34]) 2. panta 2. punktā, ja tas saskaņā ar valsts tiesību aktiem ir sodāms ar brīvības atņemšanu vai ar brīvības atņemšanu saistītu drošības līdzekli, kura maksimālais ilgums ir vismaz trīs gadi;

23) "ieceļošanas/izceļošanas sistēma" jeb "IIS" ir ieceļošanas/izceļošanas sistēma, kas izveidota ar Regulu (ES) 2017/2226;

24) "vīzu informācijas sistēma" jeb "VIS" ir vīzu informācijas sistēma, kas izveidota ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 767/2008 ([35]);

25) "Eiropas ceļošanas informācijas un atļauju sistēma" jeb "*ETIAS*" ir Eiropas ceļošanas informācijas un atļauju sistēma, kas izveidota ar Regulu (ES) 2018/1240;

([30]) Eiropas Parlamenta un Padomes Regula (ES) 2017/2226 (2017. gada 30. novembris), ar ko izveido ieceļošanas/izceļošanas sistēmu (IIS), lai reģistrētu to trešo valstu valstspiederīgo ieceļošanas un izceļošanas datus un ieceļošanas atteikumu datus, kuri šķērso dalībvalstu ārējās robežas, un ar ko paredz nosacījumus piekļuvei IIS tiesībaizsardzības nolūkos, un ar ko groza Konvenciju, ar ko īsteno Šengenas nolīgumu, un Regulas (EK) Nr. 767/2008 un (ES) Nr. 1077/2011 (OV L 327, 9.12.2017., 20. lpp.).

([31]) Padomes Lēmums 2008/633/TI (2008. gada 23. jūnijs) par izraudzīto dalībvalstu iestāžu un Eiropola piekļuvi Vīzu informācijas sistēmai (VIS) konsultāciju nolūkos, lai novērstu, atklātu un izmeklētu teroristu nodarījumus un citus smagus noziedzīgus nodarījumus (OV L 218, 13.8.2008., 129. lpp.).

([32]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1240 (2018. gada 12. septembris), ar ko izveido Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*) un groza Regulas (ES) Nr. 1077/2011, (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/1624 un (ES) 2017/2226 (OV L 236, 19.9.2018., 1. lpp.).

([33]) 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.).

([34]) 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.).

([35]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 767/2008 (2008. gada 9. jūlijs) par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (VIS regula) (OV L 218, 13.8.2008., 60. lpp.).

26) "*Eurodac*" ir *Eurodac*, kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 603/2013 ([36]);

27) "Šengenas informācijas sistēma" jeb "*SIS*" ir Šengenas Informācijas sistēma, kas izveidota ar Regulām (ES) 2018/1860, (ES) 2018/1861 un (ES) 2018/1862;

28) "*ECRIS-TCN*" ir centralizētā sistēma, ar ko apzina dalībvalstis, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un kas izveidota ar Regulu (ES) 2019/816.

5. pants

Nediskriminēšana un pamattiesības

Personas datu apstrāde, ko veic šīs regulas vajadzībām, neizraisa nekādu diskrimināciju pret personām, arī ne tādu iemeslu dēļ kā dzimums, rase, ādas krāsa, etniskā vai sociālā izcelsme, ģenētiskās īpatnības, valoda, reliģija vai pārliecība, politiski vai citi uzskati, piederība pie nacionālas minoritātes, īpašums, izcelsme, invaliditāte, vecums vai seksuālā orientācija. Tā pilnībā respektē cilvēka cieņu un integritāti, kā arī pamattiesības, tostarp tiesības uz privāto dzīvi un personas datu aizsardzību. Īpašu uzmanību pievērš bērniem, veciem cilvēkiem, personām ar invaliditāti un personām, kurām ir nepieciešama starptautiskā aizsardzība. Primāri ņem vērā bērna intereses.

II NODAĻA

Eiropas meklēšanas portāls

6. pants

Eiropas meklēšanas portāls

1. Tiek izveidots Eiropas meklēšanas portāls (*ESP*), lai atvieglotu dalībvalstu iestāžu un Savienības aģentūru ātru, netraucētu, efektīvu, sistemātisku un kontrolētu piekļuvi ES informācijas sistēmām, Eiropola datiem un Interpola datubāzēm to uzdevumu veikšanai un saskaņā ar to piekļuves tiesībām, un IIS, VIS, *ETIAS*, *Eurodac*, *SIS*, un *ECRIS-TCN* mērķiem un nolūkiem.

2. *ESP* veido:

a) centrāla infrastruktūra, tostarp meklēšanas portāls, kas ļauj vienlaikus veikt vaicājumus IIS, VIS, *ETIAS*, *Eurodac*, *SIS*, *ECRIS-TCN*, kā arī Eiropola datos un Interpola datubāzēs;

b) drošs komunikāciju kanāls starp *ESP*, dalībvalstīm un Savienības aģentūrām, kurām ir tiesības izmantot *ESP*;

c) droša komunikāciju infrastruktūra starp *ESP* un IIS, VIS, *ETIAS*, *Eurodac*, centrālo *SIS*, *ECRIS-TCN*, Eiropola datiem un Interpola datubāzēm, kā arī starp *ESP* un *CIR* un *MID* centrālajām infrastruktūrām.

3. *eu-LISA* izstrādā *ESP* un nodrošina tā tehnisko pārvaldību.

7. pants

Eiropas meklēšanas portāla izmantošana

1. *ESP* izmantošana ir atļauta tikai dalībvalstu iestādēm un Savienības aģentūrām, kurām ir piekļuve vismaz vienai no ES informācijas sistēmām saskaņā ar tiesību instrumentiem, kas reglamentē minētās ES informācijas sistēmas, *CIR* un *MID* saskaņā ar šo regulu, Eiropola datiem saskaņā ar Regulu (ES) 2016/794 vai Interpola datubāzēm saskaņā ar Savienības vai valsts tiesību aktiem, kas reglamentē šādu piekļuvi.

Minētās dalībvalstu iestādes un Savienības aģentūras var izmantot *ESP* un tā sniegtos datus tikai tiem mērķiem un nolūkiem, kas ir paredzēti tiesību instrumentos, kuri reglamentē minētās ES informācijas sistēmas, Regulā (ES) 2016/794 un šajā regulā.

([36]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 603/2013 (2013. gada 26. jūnijs) par pirkstu nospiedumu salīdzināšanas sistēmas *Eurodac* izveidi, lai efektīvi piemērotu Regulu (ES) Nr. 604/2013, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm, un par dalībvalstu tiesībaizsardzības iestāžu un Eiropola pieprasījumiem veikt salīdzināšanu ar *Eurodac* datiem tiesībaizsardzības nolūkos, un ar kuru groza Regulu (ES) Nr. 1077/2011, ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (OV L 180, 29.6.2013., 1. lpp.).

2. Šā panta 1. punktā minētās dalībvalstu iestādes un Savienības aģentūras izmanto *ESP*, lai saskaņā ar savām piekļuves tiesībām, kā minēts šo ES informācijas sistēmu reglamentējošos tiesību instrumentos un valsts tiesību aktos, *Eurodac* un *ECRIS-TCN* centrālajās sistēmās meklētu ar personām vai viņu ceļošanas dokumentiem saistītus datus. Tās izmanto *ESP* arī, lai saskaņā ar to piekļuves tiesībām, atbilstīgi šai regulai 20., 21. un 22. pantā minētajos nolūkos veiktu vaicājumus *CIR*.

3. Šā panta 1. punktā minētās dalībvalstu iestādes var izmantot *ESP*, lai centrālajā *SIS* meklētu ar personām vai viņu ceļošanas dokumentiem saistītus datus, kas minēti Regulās (ES) 2018/1860 un (ES) 2018/1861.

4. Ja to paredz Savienības tiesību akti, 1. punktā minētās Savienības aģentūras izmanto *ESP*, lai centrālajā *SIS* meklētu ar personām vai viņu ceļošanas dokumentiem saistītus datus.

5. Šā panta 1. punktā minētās dalībvalstu iestādes un Savienības aģentūras var izmantot *ESP*, lai saskaņā ar savām piekļuves tiesībām, kas paredzētas Savienības un valsts tiesību aktos, Eiropola datos meklētu ar personām vai viņu ceļošanas dokumentiem saistītus datus.

8. pants

Eiropas meklēšanas portāla lietotāju profili

1. Lai varētu izmantot *ESP*, *eu-LISA* sadarbībā ar dalībvalstīm saskaņā ar 2. punktā minētajiem tehniskajiem parametriem un piekļuves tiesībām izveido profilu, kas balstīts uz katru *ESP* lietotāju kategoriju un uz vaicājumu nolūkiem. Katrs profils saskaņā ar Savienības un valsts tiesību aktiem ietver šādu informāciju:

a) vaicājumu veikšanai izmantojamos datu laukus;

b) ES informācijas sistēmas, Eiropola datus un Interpola datubāzes, kurās veicami vaicājumi, kurās var tikt veikti vaicājumi un kurām jāsniedz atbilde lietotājam;

c) konkrētos ES informācijas sistēmu, Eiropola datu un Interpola datubāzu datus, kuros var veikt vaicājumus;

d) datu kategorijas, kas var būt sniegti katrā atbildē.

2. Komisija pieņem īstenošanas aktus, lai precizētu 1. punktā minēto profilu tehniskos parametrus saskaņā ar *ESP* lietotāju piekļuves tiesībām atbilstīgi ES informācijas sistēmas reglamentējošiem tiesību instrumentiem un valsts tiesību aktiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

3. *eu-LISA* sadarbībā ar dalībvalstīm 1. punktā minētos profilus regulāri – vismaz reizi gadā – pārskata un vajadzības gadījumā atjaunina.

9. pants

Vaicājumi

1. *ESP* lietotāji veic vaicājumu, ievadot burtciparu vai biometriskos datus *ESP*. Ja vaicājums ir veikts, *ESP* ar lietotāja iesniegtajiem datiem un atbilstīgi lietotāja profilam vienlaikus veic vaicājumu IIS, *ETIAS*, VIS, *SIS*, *Eurodac*, *ECRIS-TCN*, *CIR*, Eiropola datos un Interpola datubāzēs.

2. Datu kategorijas, kuras izmanto, lai veiktu vaicājumu, izmantojot *ESP*, atbilst tām ar personām vai ceļošanas dokumentiem saistītajām datu kategorijām, kuras var izmantot, lai veiktu vaicājumus dažādās ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs saskaņā ar tos reglamentējošajiem tiesību instrumentiem.

3. *eu-LISA* sadarbībā ar dalībvalstīm ievieš saskarnes kontroldokumentu, kura pamatā ir 38. pantā minētais *UMF* attiecībā uz *ESP*.

4. Ja *ESP* lietotājs ir veicis vaicājumu, IIS, *ETIAS*, VIS, *SIS*, *Eurodac*, *ECRIS-TCN*, *CIR*, *MID*, Eiropola dati un Interpola datubāzes atbildē uz vaicājumu sniedz tajos esošos datus.

Neskarot 20. pantu, *ESP* sniegtajā atbildē norāda, kurai ES informācijas sistēmai vai datubāzei dati pieder.

ESP nesniedz informāciju par datiem ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs, kuriem lietotājam nav piekļuves atbilstīgi piemērojamajiem Savienības un valsts tiesību aktiem.

5. Visus vaicājumus Interpola datubāzēs, kas veikti ar *ESP*, veic tā, ka Interpola brīdinājuma īpašniekam netiek atklāta nekāda informācija.

6. *ESP* atbildes lietotājam sniedz, tiklīdz ir pieejami dati no kādas ES informācijas sistēmas, Eiropola datiem vai Interpola datubāzēm. Minētajās atbildēs ietver tikai tādus datus, kuriem lietotājam ir piekļuve saskaņā ar Savienības un valsts tiesību aktiem.

7. Komisija pieņem īstenošanas aktu, lai precizētu tehnisko procedūru, kā *ESP* veic vaicājumus ES informācijas sistēmās, Eiropola datos un Interpola datubāzēs, un *ESP* atbilžu formātu. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

10. pants

Reģistra ierakstu glabāšana

1. Neskarot Regulas (ES) 2018/1862 12. un 18. pantu, Regulas (ES) 2019/816 29. pantu un Regulas (ES) 2016/794 40. pantu, *eu-LISA* glabā reģistra ierakstus par visām *ESP* ietvaros veiktajām datu apstrādes darbībām. Minētie reģistra ieraksti satur šādu informāciju:

a) dalībvalsts iestāde vai Savienības aģentūra, kas veikusi vaicājumu, un izmantotais *ESP* profils;

b) vaicājuma datums un laiks;

c) ES informācijas sistēmas un Eiropola dati, kuros veikts vaicājums.

2. Katra dalībvalsts glabā reģistra ierakstus par vaicājumiem, ko veic tās iestādes un minēto iestāžu darbinieki, kuri ir pienācīgi pilnvaroti izmantot *ESP*. Katra Savienības aģentūra glabā reģistra ierakstus par vaicājumiem, ko veic tās darbinieki, kuri ir pienācīgi pilnvaroti.

3. Reģistra ierakstus, kas minēti 1. un 2. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām minētie reģistra ieraksti vairs nav vajadzīgi.

11. pants

Alternatīvās procedūras gadījumā, ja Eiropas meklēšanas portālu tehniski nav iespējams izmantot

1. Ja *ESP* nedarbošanās dēļ tehniski to nav iespējams izmantot, lai veiktu vaicājumu vienā vai vairākās ES informācijas sistēmās vai *CIR*, *eu-LISA* automatizēti informē *ESP* lietotājus.

2. Ja *ESP* tehniski nav iespējams izmantot, lai veiktu vaicājumu vienā vai vairākās ES informācijas sistēmās vai *CIR*, jo kādā dalībvalstī nedarbojas valsts infrastruktūra, minētā dalībvalsts automatizēti informē *eu-LISA* un Komisiju.

3. Šā panta 1. vai 2. punktā minētajos gadījumos – un līdz tehniskās kļūmes novēršanai – nepiemēro 7. panta 2. un 4. punktā minēto pienākumu un dalībvalstis tieši piekļūst ES informācijas sistēmām vai *CIR*, kad tas tām jādara atbilstīgi Savienības vai valsts tiesību aktiem.

4. Ja *ESP* tehniski nav iespējams izmantot, lai veiktu vaicājumu vienā vai vairākās ES informācijas sistēmās vai *CIR*, jo nedarbojas kādas Savienības aģentūras infrastruktūra, minētā aģentūra automatizēti informē *eu-LISA* un Komisiju.

III NODAĻA

Kopējs biometrisko datu salīdzināšanas pakalpojums

12. pants

Kopējs biometrisko datu salīdzināšanas pakalpojums

1. Tiek izveidots kopējs biometrisko datu salīdzināšanas pakalpojums (kopējais *BMS*), kas glabā biometriskās veidnes, kuras iegūtas no 13. pantā minētajiem *CIR* un *SIS* glabātajiem biometriskajiem datiem, un kas ļauj veikt biometrisko datu vaicājumus vairākās ES informācijas sistēmās, lai atbalstītu *CIR* un *MID* darbību un palīdzētu sasniegt IIS, VIS, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

2. Kopējo *BMS* veido:

a) centrāla infrastruktūra, kas aizstāj attiecīgi IIS, VIS, *SIS*, *Eurodac* un *ECRIS-TCN* centrālās sistēmas, ciktāl tā glabā biometriskās veidnes un dod iespēju meklēt ar biometriskajiem datiem;

b) droša komunikāciju infrastruktūra starp kopējo *BMS*, centrālo *SIS* un *CIR*.

3. *eu-LISA* izstrādā kopējo *BMS* un nodrošina tā tehnisko pārvaldību.

13. pants

Biometrisko veidņu glabāšana kopējā biometrisko datu salīdzināšanas pakalpojumā

1. Kopējā *BMS* glabā biometriskās veidnes, kuras tas iegūst no šādiem biometriskajiem datiem:

a) dati, kas minēti Regulas (ES) 2018/1862 20. panta 3. punkta w) un y) apakšpunktā, izņemot plaukstas nospiedumu datus;

b) dati, kas minēti Regulas (ES) 2019/816 5. panta 1. punkta b) apakšpunktā un 2. punktā.

Biometriskās veidnes glabā kopējā *BMS* loģiski nodalītas atbilstīgi ES informācijas sistēmai, no kuras dati ir iegūti.

2. Attiecībā uz katru 1. punktā minēto datu kopu kopējais *BMS* katrā biometriskajā veidnē ietver atsauci uz ES informācijas sistēmām, kurās attiecīgie biometriskie dati tiek glabāti un atsauci uz faktiskajiem ierakstiem minētajās ES informācijas sistēmās.

3. Biometriskās veidnes tiek ievadītas kopējā *BMS* tikai pēc automatizētas vienai no ES informācijas sistēmām pievienoto biometrisko datu kvalitātes pārbaudes, ko veic kopējais *BMS*, lai pārliecinātos, ka ir ievērots datu kvalitātes minimuma standarts.

4. Šā panta 1. punktā minēto datu glabāšana atbilst 37. panta 2. punktā minētajiem kvalitātes standartiem.

5. Komisija ar īstenošanas aktu nosaka veiktspējas prasības un praktisko kārtību, kā uzraudzīt kopējā *BMS* veiktspēju, lai nodrošinātu, ka biometrisko meklējumu efektivitāte ir pietiekama procedūrām, kurās ir izšķirīgs laiks, piemēram, robežpārbaudēm un identifikācijai. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

14. pants

Biometrisko datu meklēšana ar kopējā biometrisko datu salīdzināšanas pakalpojuma palīdzību

Lai meklētu *CIR* un *SIS* glabātos biometriskos datus, *CIR* un *SIS* izmanto biometriskās veidnes, kas tiek glabātas kopējā *BMS*. Vaicājumus ar biometriskajiem datiem veic saskaņā ar mērķiem, kas paredzēti šajā regulā un Regulās (EK) Nr. 767/2008, (ES) 2017/2226, (ES) 2018/1860, (ES) 2018/1861, (ES) 2018/1862 un (ES) 2019/816.

15. pants

Datu saglabāšana kopējā biometrisko datu salīdzināšanas pakalpojumā

Datus, kas minēti 13. panta 1. un 2. punktā, glabā kopējā *BMS* tikai tik ilgi, cik ilgi atbilstošos biometriskos datus glabā *CIR* vai *SIS*. Datu dzēšanu no kopējā *BMS* veic automatizēti.

16. pants

Reģistra ierakstu glabāšana

1. Neskarot Regulas (ES) 2018/1862 12. un 18. pantu un Regulas (ES) 2019/816 29. pantu, *eu-LISA* glabā reģistra ierakstus par visām kopējā *BMS* ietvaros veiktajām datu apstrādes darbībām. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu;

b) vēsture, kas saistīta ar biometrisko veidņu izveidi un glabāšanu;

c) ES informācijas sistēmas, kurās veikti vaicājumi, izmantojot kopējā *BMS* glabātās biometriskās veidnes;

d) vaicājuma datums un laiks;

e) vaicājuma veikšanai izmantoto biometrisko datu veids;

f) vaicājuma rezultāti un rezultātu datums un laiks.

2. Katra dalībvalsts glabā reģistra ierakstus par tās iestāžu un minēto iestāžu darbinieku, kuri ir pienācīgi pilnvaroti izmantot kopējo *BMS*, veiktiem vaicājumiem. Katra Savienības aģentūra glabā reģistra ierakstus par tās pienācīgi pilnvarotu darbinieku veiktiem vaicājumiem.

3. Reģistra ierakstus, kas minēti 1. un 2. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām minētie reģistra ieraksti vairs nav vajadzīgi.

IV NODAĻA

Kopējs identitātes repozitorijs

17. pants

Kopējs identitātes repozitorijs

1. Tiek izveidots kopējs identitātes repozitorijs (*CIR*), ar kuru izveido individuālu personas datni par katru personu, kas reģistrēta IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, un kurā ir ietverti 18. pantā minētie dati, lai atvieglotu IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN* reģistrēto personu pareizu identifikāciju saskaņā ar 20. pantu, atbalstītu *MID* darbību saskaņā ar 21. pantu un atvieglotu un racionalizētu izraudzīto iestāžu un Eiropola piekļuvi IIS, VIS, *ETIAS* un *Eurodac*, ja tas vajadzīgs, lai novērstu, atklātu vai izmeklētu teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus saskaņā ar 22. pantu.

2. *CIR* veido:

a) centrāla infrastruktūra, kas aizstāj attiecīgi IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN* centrālās sistēmas, ciktāl tā glabā 18. pantā minētos datus;

b) drošs komunikāciju kanāls starp *CIR*, dalībvalstīm un Savienības aģentūrām, kurām ir tiesības izmantot *CIR* saskaņā ar Savienības un valsts tiesību aktiem;

c) droša komunikāciju infrastruktūra starp *CIR* un IIS, VIS, *ETIAS*, *Eurodac* un *ECRIS-TCN*, kā arī ar *ESP*, kopējā *BMS* un *MID* centrālajām infrastruktūrām.

3. *eu-LISA* izstrādā *CIR* un nodrošina tā tehnisko pārvaldību.

4. Ja *CIR* tehnisku problēmu dēļ nav iespējams veikt vaicājumu *CIR*, lai identificētu personu saskaņā ar 20. pantu, konstatētu vairākas identitātes saskaņā ar 21. pantu vai novērstu, atklātu vai izmeklētu teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus saskaņā ar 22. pantu, *eu-LISA* automatizēti informē *CIR* lietotājus.

5. *eu-LISA* sadarbībā ar dalībvalstīm ievieš saskarnes kontroldokumentu, kura pamatā ir 38. pantā minētais *UMF* attiecībā uz *CIR*.

18. pants

Kopējā identitātes repozitorija dati

1. *CIR* glabā šādus datus, kas loģiski nodalīti atbilstīgi tai informācijas sistēmai, no kuras dati tika iegūti: dati, kas minēti Regulas (ES) 2019/816 5. panta 1. punkta b) apakšpunktā un 2. punktā, un šādi dati, kuri uzskaitīti tās 5. panta 1. punkta a) apakšpunktā: uzvārds, vārdi, dzimšanas datums, dzimšanas vieta (pilsēta un valsts), valstspiederība vai valstspiederības; dzimums, attiecīgā gadījumā iepriekšējie vārdi, pseidonīmi vai pieņemtie vārdi, ja tādi ir pieejami, kā arī informācija par ceļošanas dokumentiem, ja tāda ir pieejama.

2. Attiecībā uz katru datu kopu, kas minēta 1. punktā, *CIR* ietver atsauci uz ES informācijas sistēmām, kurām dati pieder.

3. Iestādes, kas piekļūst *CIR*, to dara saskaņā ar to piekļuves tiesībām atbilstīgi ES informācijas sistēmas reglamentējošiem tiesību instrumentiem un valsts tiesību aktiem, un saskaņā ar to piekļuves tiesībām atbilstīgi šai regulai 20., 21. un 22. pantā minētajos nolūkos.

4. Attiecībā uz katru datu kopu, kas minēta 1. punktā, *CIR* ietver atsauci uz faktisko ierakstu ES informācijas sistēmās, kurām dati pieder.

5. Šā panta 1. punktā minēto datu glabāšana atbilst 37. panta 2. punktā minētajiem kvalitātes standartiem.

19. pants

Kopējā identitātes repozitorijā ietverto datu papildināšana, grozīšana un dzēšana

1. Ja *Eurodac* vai *ECRIS-TCN* ietvertie dati tiek papildināti, grozīti vai dzēsti, tad 18. pantā minētos datus, kas glabājas *CIR* personas datnē, automatizēti atbilstoši papildina, groza vai dzēš.

2. Ja *MID* saskaņā ar 32. vai 33. pantu ir izveidota balta vai sarkana saikne starp *CIR* veidojošo divu vai vairāku ES informācijas sistēmu datiem, *CIR* nevis izveido jaunu personas datni, bet pievieno jaunos datus ar saikni saistīto datu personas datnei.

20. pants

Piekļuve kopējam identitātes repozitorijam identifikācijas nolūkā

1. *CIR* vaicājumus veic policijas iestāde saskaņā ar 2. un 5. punktu tikai šādos apstākļos:

a) ja policijas iestāde nespēj identificēt personu, jo trūkst ceļošanas dokumenta vai cita ticama dokumenta, kas apliecinātu personas identitāti;

b) ja ir šaubas par attiecīgas personas sniegtajiem identitātes datiem;

c) ja ir šaubas par attiecīgas personas iesniegtā ceļošanas dokumenta vai cita ticama dokumenta autentiskumu;

d) ja ir šaubas par ceļošanas dokumenta vai cita ticama dokumenta turētāja identitāti; vai

e) ja persona nespēj vai atsakās sadarboties.

Šādi vaicājumi nav atļauti attiecībā uz nepilngadīgajiem, kas jaunāki par 12 gadiem, izņemot, ja tas ir bērna interesēs.

2. Ja iestājas kāds no 1. punktā minētajiem apstākļiem un policijas iestāde ir pilnvarota ar valsts leģislatīviem pasākumiem, kā minēts 5. punktā, tā – vienīgi personas identifikācijas nolūkos – var veikt vaicājumu *CIR*, izmantojot minētās personas biometriskos datus, kuri iegūti tiešā veidā identitātes pārbaudes laikā, ar noteikumu, ka šī procedūra sākta minētās personas klātbūtnē.

3. Ja vaicājuma rezultātā noskaidrojas, ka dati par minēto personu tiek glabāti *CIR*, policijas iestādei ir piekļuve aplūkot 18. panta 1. punktā minētos datus.

Ja personas biometriskie dati nav izmantojami vai ja vaicājums uz šo datu pamata neizdodas, vaicājumu veic, izmantojot personas identitātes datus apvienojumā ar ceļošanas dokumenta datiem, vai izmantojot identitātes datus, kurus sniegusi minētā persona.

4. Ja policijas iestāde ir pilnvarota ar valsts leģislatīviem pasākumiem, kā minēts 6. punktā, tā – vienīgi nolūkā identificēt nezināmas personas, kuras nespēj sevi identificēt, vai neidentificētas cilvēku mirstīgās atliekas dabas katastrofas, nelaimes gadījuma vai teroristu uzbrukuma gadījumā – var veikt vaicājumu *CIR*, izmantojot minēto personu biometriskos datus.

5. Dalībvalstis, kas vēlas izmantot 2. punktā paredzēto iespēju, pieņem valsts leģislatīvos pasākumus. To darot, dalībvalstis ņem vērā, ka ir jāizvairās no jebkādas trešo valstu valstspiederīgo diskriminācijas. Ar šādiem leģislatīviem pasākumiem konkretizē precīzos identifikācijas mērķus atbilstīgi 2. panta 1. punkta b) un c) apakšpunktā minētajiem mērķiem. Minētās dalībvalstis izraugās kompetentās policijas iestādes un nosaka šādu pārbaužu procedūras, nosacījumus un kritērijus.

6. Dalībvalstis, kas vēlas izmantot 4. punktā paredzēto iespēju, pieņem valsts leģislatīvos pasākumus, kuros noteiktas procedūras, nosacījumi un kritēriji.

21. pants

Piekļuve kopējam identitātes repozitorijam vairāku identitāšu konstatēšanas nolūkā

1. Ja *CIR* vaicājuma rezultāts ir dzeltena saikne atbilstoši 28. panta 4. punktam, tad iestādei, kas atbild par atšķirīgu identitāšu manuālu verifikāciju saskaņā ar 29. pantu, vienīgi šīs verifikācijas veikšanas nolūkā ir piekļuve 18. panta 1. un 2. punktā minētajiem *CIR* glabātajiem datiem, kuri ir saistīti ar dzeltenu saikni.

2. Ja *CIR* vaicājuma rezultāts ir sarkana saikne atbilstoši 32. pantam, tad 26. panta 2. punktā minētajām iestādēm vienīgi identitātes viltošanas apkarošanas nolūkos ir piekļuve 18. panta 1. un 2. punktā minētajiem *CIR* glabātajiem datiem, kuri ir saistīti ar sarkanu saikni.

22. pants

Vaicājumi kopējā identitātes repozitorijā nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus

1. Ja kādā konkrētā lietā ir pamatots iemesls uzskatīt, ka ES informācijas sistēmu aplūkošana palīdzēs novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, jo īpaši tad, ja ir aizdomas, ka teroristu nodarījumā vai citos smagos noziedzīgos nodarījumos aizdomās turamais, vainīgais vai cietušais ir persona, kuras dati tiek glabāti *Eurodac*, izraudzītās iestādes un Eiropols var aplūkot *CIR*, lai iegūtu informāciju, vai dati par konkrētu personu atrodas *Eurodac*.

2. Ja atbildē uz vaicājumu *CIR* norāda, ka dati par minēto personu atrodas *Eurodac*, *CIR* sniedz izraudzītajām iestādēm un Eiropolam atbildi atsauces veidā, kā minēts 18. panta 2. punktā, norādot, ka *Eurodac* ir ietverti vaicājumam atbilstīgie dati. *CIR* atbild tā, lai netiktu apdraudēta datu drošība.

Atbildi, kurā ir norādīts, ka dati par minēto personu ir atrodami *Eurodac*, izmanto tikai pilnīgas piekļuves pieprasījuma iesniegšanas nolūkiem, ievērojot nosacījumus un procedūras, kas ir noteiktas tiesību instrumentā, kurš reglamentē šādu piekļuvi.

Atbilstības vai vairāku atbilstību gadījumā izraudzītā iestāde vai Eiropols pieprasa pilnīgu piekļuvi vismaz vienai no informācijas sistēmām, no kuras tika ģenerēta atbilstība.

Ja izņēmuma gadījumā šāda pilnīga piekļuve netiek pieprasīta, izraudzītās iestādes reģistrē pamatojumu pieprasījuma neveikšanai, kas ir izsekojams līdz valsts datnei. Eiropols pamatojumu reģistrē attiecīgajā datnē.

3. Pilnīga piekļuve *Eurodac* ietvertajiem datiem nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus joprojām ir pakļauta nosacījumiem un procedūrām, kas izklāstīti tiesību instrumentā, kurš reglamentē šādu piekļuvi.

23. pants

Datu saglabāšana kopējā identitātes repozitorijā

1. Datus, kas minēti 18. panta 1., 2. un 4. punktā, automatizēti dzēš no *CIR* saskaņā ar datu saglabāšanas noteikumiem, kuri paredzēti Regulā (ES) 2019/816.

2. Personas datni glabā *CIR* tikai tik ilgi, cik ilgi atbilstošie dati tiek glabāti vismaz vienā no ES informācijas sistēmām, kuru dati ir ietverti *CIR*. Saiknes izveide neietekmē katra saistīto datu elementa saglabāšanas laikposmu.

24. pants

Reģistra ierakstu glabāšana

1. Neskarot Regulas (ES) 2019/816 29. pantu, *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām saskaņā ar šā panta 2., 3. un 4. punktu.

2. *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām, ievērojot 20. pantu. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu;

b) tā lietotāja piekļuves nolūks, kurš veic vaicājumu ar *CIR* starpniecību;

c) vaicājuma datums un laiks;

d) vaicājuma veikšanai izmantoto datu veids;

e) vaicājuma rezultāti.

3. *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām, ievērojot 21. pantu. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu;

b) tā lietotāja piekļuves nolūks, kurš veic vaicājumu ar *CIR* starpniecību;

c) vaicājuma datums un laiks;

d) ja ir izveidota saikne – vaicājuma veikšanai izmantotie dati un vaicājuma rezultāti, kas norāda ES informācijas sistēmu, no kuras dati tika saņemti.

4. *eu-LISA* glabā reģistra ierakstus par visām *CIR* ietvaros veiktajām datu apstrādes darbībām, ievērojot 22. pantu. Minētie reģistra ieraksti ietver šādu informāciju:

a) vaicājuma datums un laiks;

b) vaicājuma veikšanai izmantotie dati;

c) vaicājuma rezultāti;

d) dalībvalsts vai Savienības aģentūra, kas veic vaicājumu *CIR*.

Kompetentā uzraudzības iestāde saskaņā ar Direktīvas (ES) 2016/680 41. pantu vai Eiropas Datu aizsardzības uzraudzītājs saskaņā ar Regulas (ES) 2016/794 43. pantu ne retāk kā reizi sešos mēnešos regulāri verificē reģistra ierakstus par šādu piekļuvi, lai pārbaudītu, vai ir ievērotas šīs regulas 22. panta 1.un 2. punktā noteiktās procedūras un nosacījumi.

5. Katra dalībvalsts glabā reģistra ierakstus par vaicājumiem, ko tās iestādes un minēto iestāžu darbinieki, kuri ir pienācīgi pilnvaroti izmantot *CIR*, veic saskaņā ar 20., 21. un 22. pantu. Katra Savienības aģentūra glabā reģistra ierakstus par vaicājumiem, ko tās pienācīgi pilnvaroti darbinieki veic saskaņā ar 21. un 22. pantu.

Papildus tam attiecībā uz jebkādu piekļuvi *CIR* saskaņā ar 22. pantu katra dalībvalsts glabā šādus reģistra ierakstus:

a) atsauce uz valsts datni;

b) piekļuves nolūks;

c) saskaņā ar valsts noteikumiem – tās amatpersonas unikālā lietotāja identitāte, kura veica vaicājumu, un tās amatpersonas unikālā lietotāja identitāte, kura lika veikt vaicājumu.

6. Saskaņā ar Regulu (ES) 2016/794 Eiropols par jebkādu piekļuvi *CIR*, ko piešķir atbilstoši šīs regulas 22. pantam, glabā reģistra ierakstus par tās amatpersonas unikālo lietotāja identitāti, kura veica vaicājumu, un tās amatpersonas unikālo lietotāja identitāti, kura lika veikt vaicājumu.

7. Reģistra ierakstus, kas minēti 2. līdz 6. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām minētie reģistra ieraksti vairs nav vajadzīgi.

8. *eu-LISA* glabā reģistra ierakstus, kas saistīti ar personas datnēs glabāto datu vēsturi. *eu-LISA* šādus reģistra ierakstus automatizēti dzēš, kolīdz dati ir dzēsti.

V NODAĻA

Vairāku identitāšu detektors

25. pants

Vairāku identitāšu detektors

1. Tiek izveidots vairāku identitāšu detektors (*MID*), ar kuru izveido un glabā 34. pantā minētās identitātes apstiprinājuma datnes, kas satur saiknes starp datiem ES informācijas sistēmās, kuras ir iekļautas *CIR* un *SIS* un kas ļauj konstatēt vairākas identitātes, nolūkā sasniegt divējādu mērķi, proti, atvieglot identitātes pārbaudes un apkarot identitātes viltošanu, lai atbalstītu *CIR* darbību un palīdzētu sasniegt IIS, VIS, *ETIAS*, *Eurodac*, *SIS* un *ECRIS-TCN* mērķus.

2. *MID* veido:

a) centrāla infrastruktūra, kas glabā saiknes un atsauces uz ES informācijas sistēmām;

b) droša komunikāciju infrastruktūra, kuras mērķis ir savienot *MID* ar *SIS* un centrālajām *ESP* un *CIR* infrastruktūrām.

3. *eu-LISA* izstrādā *MID* un nodrošina tā tehnisko pārvaldību.

26. pants

Piekļuve vairāku identitāšu detektoram

1. Lai veiktu atšķirīgu identitāšu manuālu verifikāciju, kas minēta 29. pantā, piekļuvi 34. pantā minētajiem datiem, kas tiek glabāti *MID*, piešķir:

a) tās dalībvalsts *SIRENE* birojam, kura izveido vai atjaunina brīdinājumu saskaņā ar Regulu (ES) 2018/1862;

b) notiesāšanas dalībvalsts centrālajām iestādēm brīdī, kad *ECRIS-TCN* reģistrē vai groza datus saskaņā ar Regulas (ES) 2019/816 5. vai 9. pantu.

2. Dalībvalsts iestādēm un Savienības aģentūrām, kurām ir piekļuve vismaz vienai *CIR* iekļautajai ES informācijas sistēmai vai kurām ir piekļuve *SIS*, ir piekļuve 34. panta a) un b) punktā minētajiem datiem attiecībā uz jebkādu sarkanu saikni, kas minēta 32. pantā.

3. Dalībvalstu iestādēm un Savienības aģentūrām ir piekļuve baltajām saiknēm, kas minētas 33. pantā, ja tām ir piekļuve abām ES informācijas sistēmām, kurās ir dati, starp kuriem izveidota baltā saikne.

4. Dalībvalstu iestādēm un Savienības aģentūrām ir piekļuve zaļajām saiknēm, kas minētas 31. pantā, ja tām ir piekļuve abām ES informācijas sistēmām, kurās ir dati, starp kuriem izveidota zaļā saikne, un vaicājums minētajās informācijas sistēmās ir atklājis atbilstību attiecībā pret abām saistīto datu kopām.

27. pants

Vairāku identitāšu konstatēšana

1. *CIR* un *SIS* veic vairāku identitāšu konstatēšanu, ja:

a) *SIS* ir izveidots vai atjaunināts brīdinājums par personu saskaņā ar Regulas (ES) 2018/1862 VI līdz IX nodaļu;

b) *ECRIS-TCN* ir izveidots vai grozīts datu ieraksts saskaņā ar Regulas (ES) 2019/816 5. vai 9. pantu.

2. Ja datos, kas ietverti kādā no 1. punktā minētajām ES informācijas sistēmām, ir biometriskie dati, tad *CIR* un centrālā *SIS* izmanto kopējo *BMS*, lai veiktu vairāku identitāšu konstatēšanu. Kopējais *BMS* salīdzina no jebkādiem jauniem biometriskiem datiem iegūtās biometriskās veidnes ar kopējā *BMS* jau ietvertajām biometriskajām veidnēm, lai pārbaudītu, vai dati, kas attiecas uz vienu un to pašu personu, jau tiek glabāti *CIR* vai centrālajā *SIS*.

3. Papildus 2. punktā minētajam procesam *CIR* un centrālā *SIS* izmanto *ESP*, lai meklētu attiecīgi *CIR* un centrālajā *SIS* glabātos datus, izmantojot šādus datus:

a) uzvārdi, vārdi, vārdi dzimšanas brīdī, iepriekš lietoti vārdi un pseidonīmi; dzimšanas vieta, dzimšanas datums, dzimums un visas valstspiederības, kā minēts Regulas (ES) 2018/1862 20. panta 3. punktā;

b) uzvārds, vārdi, dzimšanas datums, dzimšanas vieta (pilsēta un valsts), valstspiederība vai valstspiederības un dzimums, kā minēts Regulas (ES) 2019/816 5. panta 1. punkta a) apakšpunktā.

4. Papildus 2. un 3. punktā minētajam procesam *CIR* un centrālā *SIS* izmanto *ESP*, lai meklētu attiecīgi centrālajā *SIS* un *CIR* glabātos datus, izmantojot ceļošanas dokumenta datus.

5. Vairāku identitāšu konstatēšanu veic vienīgi, lai salīdzinātu vienā ES informācijas sistēmā pieejamos datus ar datiem, kas pieejami citās ES informācijas sistēmās.

28. pants

Vairāku identitāšu konstatēšanas rezultāti

1. Ja 27. panta 2., 3. un 4. punktā minētie vaicājumi neuzrāda nevienu atbilstību, tad turpina 27. panta 1. punktā minētās procedūras saskaņā ar tās reglamentējošiem tiesību instrumentiem.

2. Ja 27. panta 2., 3. un 4. punktā minētais vaicājums uzrāda vienu vai vairākas atbilstības, tad *CIR* un – vajadzības gadījumā – *SIS* izveido saikni starp vaicājuma veikšanai izmantotajiem datiem un datiem, uz kuriem attiecas atbilstība.

Ja tiek uzrādītas vairākas atbilstības, izveido saikni starp visiem datiem, uz kuriem attiecas atbilstība. Ja dati jau bija saistīti, esošo saikni paplašina, ietverot arī vaicājuma veikšanai izmantotos datus.

3. Ja 27. panta 2., 3. un 4. punktā minētais vaicājums uzrāda vienu vai vairākas atbilstības un saistīto datņu identitātes dati ir tādi paši vai līdzīgi, tad izveido baltu saikni saskaņā ar 33. pantu.

4. Ja 27. panta 2., 3. un 4. punktā minētais vaicājums uzrāda vienu vai vairākas atbilstības un saistīto datņu identitātes datus nevar uzskatīt par līdzīgiem, tad izveido dzeltenu saikni saskaņā ar 30. pantu un piemēro 29. pantā minēto procedūru.

5. Komisija pieņem deleģētos aktus saskaņā ar 69. pantu, ar ko paredz procedūras tādu gadījumu noteikšanai, kuros identitātes datus var uzskatīt par tādiem pašiem vai līdzīgiem.

6. Saiknes glabā 34. pantā minētajā identitātes apstiprinājuma datnē.

7. Komisija sadarbībā ar *eu-LISA* ar īstenošanas aktiem nosaka tehniskos noteikumus saikņu izveidošanai starp datiem no dažādām ES informācijas sistēmām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

29. pants

Atšķirīgu identitāšu manuāla verifikācija un atbildīgās iestādes

1. Neskarot 2. punktu, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir:

a) dalībvalsts *SIRENE* birojs attiecībā uz atbilstībām, kas tika uzrādītas brīdī, kad tika izveidots vai atjaunināts *SIS* brīdinājums saskaņā ar Regulu (ES) 2018/1862;

b) notiesāšanas dalībvalsts centrālās iestādes attiecībā uz atbilstībām, kas tika uzrādītas brīdī, kad *ECRIS-TCN* tika reģistrēti vai grozīti dati saskaņā ar Regulas (ES) 2019/816 5. vai 9. pantu.

MID norāda iestādi, kas ir atbildīga par atšķirīgu identitāšu manuālu verifikāciju, identitātes apstiprinājuma datnē.

2. Par atšķirīgu identitāšu manuālu verifikāciju identitātes apstiprinājuma datnē atbildīgā iestāde ir brīdinājumu izveidojušās dalībvalsts *SIRENE* birojs, ja ir izveidota saikne uz datiem, kas ir ietverti brīdinājumā par:

a) personām, ko meklē, lai apcietinātu nolūkā tās nodot vai izdot, kā minēts Regulas (ES) 2018/1862 26. pantā;

b) pazudušām personām vai neaizsargātām personām, kā minēts Regulas (ES) 2018/1862 32. pantā;

c) personām, ko cenšas atrast, lai tās varētu palīdzēt tiesas procesā, kā minēts Regulas (ES) 2018/1862 34. pantā;

d) personām diskrētu pārbaužu, izmeklēšanas pārbaužu vai īpašu pārbaužu vajadzībām, kā minēts Regulas (ES) 2018/1862 36. pantā.

3. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai iestādei ir piekļuve saistītajiem datiem, kas ietverti attiecīgajā identitātes apstiprinājuma datnē, un identitātes datiem, uz kuriem ir saikne *CIR* un – vajadzības gadījumā – *SIS*. Tā novērtē atšķirīgās identitātes nekavējoties. Tiklīdz novērtēšana ir pabeigta, tā atjaunina saikni saskaņā ar 31., 32. un 33. pantu un nekavējoties pievieno to identitātes apstiprinājuma datnei.

4. Ja ir izveidota vairāk nekā viena saikne, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde katru saikni izvērtē atsevišķi.

5. Ja dati, uz kuru pamata ir uzrādīta atbilstība, jau bija saistīti, tad par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ņem vērā esošās saiknes, izvērtējot jaunu saikņu izveidi.

30. pants

Dzeltena saikne

1. Ja atšķirīgu identitāšu manuāla verifikācija vēl nav veikta, saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā dzeltenu jebkurā no šādiem gadījumiem:

a) saistītajos datos ir vieni un tie paši biometriskie dati, bet ir līdzīgi vai atšķirīgi identitātes dati;

b) saistītajos datos ir atšķirīgi identitātes dati, bet ir vieni un tie paši ceļošanas dokumenta dati, un vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu;

c) saistītajos datos ir vieni un tie paši identitātes dati, bet ir atšķirīgi biometriskie dati;

d) saistītajos datos ir līdzīgi vai atšķirīgi identitātes dati un ir vieni un tie paši ceļošanas dokumenta dati, bet ir atšķirīgi biometriskie dati.

2. Ja saikne ir klasificēta kā dzeltena saskaņā ar 1. punktu, tad piemēro 29. pantā noteikto procedūru.

31. pants

Zaļa saikne

1. Saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā zaļu, ja:

a) saistītajos datos ir atšķirīgi biometriskie dati, bet ir vieni un tie paši identitātes dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām;

b) saistītajos datos ir atšķirīgi biometriskie dati, ir līdzīgi vai atšķirīgi identitātes dati un ir vieni un tie paši ceļošanas dokumenta dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām;

c) saistītajos datos ir atšķirīgi identitātes dati, bet ir vieni un tie paši ceļošanas dokumenta dati, vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām.

2. Ja veic vaicājumu *CIR* vai *SIS* un ir iegūta zaļa saikne starp datiem divās vai vairākās ES informācijas sistēmās, tad *MID* norāda, ka saistīto datu identitātes dati neatbilst vienai un tai pašai personai.

3. Ja kādas dalībvalsts iestādes rīcībā ir pierādījumi, ka zaļā saikne ir nepareizi reģistrēta *MID*, ka zaļā saikne nav atjaunināta vai ka dati ir apstrādāti *MID* vai ES informācijas sistēmās, pārkāpjot šo regulu, tā pārbauda attiecīgos datus, kas glabājas *CIR* un *SIS*, un vajadzības gadījumā nekavējoties izlabo vai izdzēš minēto saikni no *MID*. Minētā dalībvalsts iestāde nekavējoties informē dalībvalsti, kas ir atbildīga par atšķirīgu identitāšu manuālu verifikāciju.

32. pants

Sarkana saikne

1. Saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā sarkanu jebkurā no šādiem gadījumiem:

a) saistītajos datos ir vieni un tie paši biometriskie dati, bet ir līdzīgi vai atšķirīgi identitātes dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati nepamatoti attiecas uz vienu un to pašu personu;

b) saistītajos datos ir vieni un tie paši, līdzīgi vai atšķirīgi identitātes dati un vieni un tie paši ceļošanas dokumenta dati, bet atšķirīgi biometriskie dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati attiecas uz divām dažādām personām, no kurām vismaz viena nepamatoti izmanto vienu un to pašu ceļošanas dokumentu;

c) saistītajos datos ir vieni un tie paši identitātes dati, bet ir atšķirīgi biometriskie dati un atšķirīgi ceļošanas dokumenta dati – vai tādu nemaz nav –, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati nepamatoti attiecas uz divām dažādām personām;

d) saistītajos datos ir atšķirīgi identitātes dati, bet ir vieni un tie paši ceļošanas dokumenta dati, vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati nepamatoti attiecas uz vienu un to pašu personu.

2. Ja veic vaicājumu *CIR* vai *SIS* un ir iegūta sarkana saikne starp datiem divās vai vairākās ES informācijas sistēmās, tad *MID* norāda 34. pantā minētos datus. Turpmākos pasākumus sarkanas saiknes gadījumā veic saskaņā ar Savienības un valsts tiesību aktiem, jebkādas juridiskās sekas attiecīgajai personai balstot tikai uz atbilstīgajiem datiem par minēto personu. Tikai sarkanas saiknes pastāvēšana vien nerada attiecīgajai personai nekādas juridiskas sekas.

3. Ja ir izveidota sarkana saikne starp datiem no IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, *CIR* glabāto personas datni atjaunina saskaņā ar 19. panta 2. punktu.

4. Neskarot Regulās (ES) 2018/1860, (ES) 2018/1861 un (ES) 2018/1862 minētos noteikumus par brīdinājumu apstrādi *SIS* un neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību un sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta nekāda valsts veikta izmeklēšana, gadījumos, kad ir izveidota sarkana saikne, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde informē attiecīgo personu par vairāku nelikumīgu identitātes datu esamību un sniedz personai vienotu identifikācijas numuru, kas minēts šīs regulas 34. panta c) punktā, atsauci uz iestādi, kas atbild par atšķirīgo identitāšu manuālu verifikāciju un minēta šīs regulas 34. panta d) punktā, un saskaņā ar šīs regulas 49. pantu izveidotā tīmekļa portāla tīmekļa adresi.

5. Par atšķirīgo identitāšu manuālu verifikāciju atbildīgā iestāde sniedz 4. punktā minēto informāciju rakstiski standarta veidlapā. Komisija ar īstenošanas aktiem nosaka minētās veidlapas saturu un izklāstu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

6. Ja ir izveidota sarkana saikne, *MID* automatizēti informē iestādes, kas atbild par saistītajiem datiem.

7. Ja dalībvalsts iestādei vai Savienības aģentūrai, kurai ir piekļuve *CIR* vai *SIS*, ir pierādījumi, kas liecina, ka sarkana saikne ir nepareizi reģistrēta *MID* vai ka *MID*, *CIR* vai *SIS* dati ir apstrādāti, pārkāpjot šo regulu, minētā iestāde vai aģentūra pārbauda attiecīgos *CIR* vai *SIS* glabātos datus un:

a) ja saikne attiecas uz kādu no 29. panta 2. punktā minētajiem *SIS* brīdinājumiem, nekavējoties informē tās dalībvalsts attiecīgo *SIRENE* biroju, kura izveidojusi minēto *SIS* brīdinājumu;

b) visos citos gadījumos nekavējoties labo vai dzēš saikni no *MID*.

Ja ar *SIRENE* biroju sazinās, ievērojot pirmās daļas a) punktu, tas pārbauda dalībvalsts iestādes vai Savienības aģentūras sniegtos pierādījumus un attiecīgā gadījumā nekavējoties labo vai dzēš saikni no *MID*.

Dalībvalsts iestāde, kas ieguvusi pierādījumus, nekavējoties informē par atšķirīgu identitāšu manuālu verifikāciju atbildīgo dalībvalsts iestādi par jebkuru attiecīgu sarkanas saiknes labošanu vai dzēšanu.

33. pants

Balta saikne

1. Saikni starp datiem no divām vai vairākām ES informācijas sistēmām klasificē kā baltu jebkurā no šādiem gadījumiem:

a) saistītajos datos ir vieni un tie paši biometriskie dati un vieni un tie paši vai līdzīgi identitātes dati;

b) saistītajos datos ir vieni un tie paši vai līdzīgi identitātes dati, vieni un tie paši ceļošanas dokumenta dati, un vismaz vienā no ES informācijas sistēmām nav attiecīgās personas biometrisko datu;

c) saistītajos datos ir vieni un tie paši biometriskie dati, vieni un tie paši ceļošanas dokumenta dati un līdzīgi identitātes dati;

d) saistītajos datos ir vieni un tie paši biometriskie dati, bet ir līdzīgi vai atšķirīgi identitātes dati, un par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde ir secinājusi, ka saistītie dati pamatoti attiecas uz vienu un to pašu personu.

2. Ja veic vaicājumu *CIR* vai *SIS* un pastāv balta saikne starp datiem divās vai vairākās ES informācijas sistēmās, tad *MID* norāda, ka saistīto datu identitātes dati atbilst vienai un tai pašai personai. ES informācijas sistēmas, kurās veikts vaicājums, sniedz atbildi, vajadzības gadījumā norādot visus saistītos datus par attiecīgo personu un tādējādi izraisot atbilstību datiem, kas ir saistīti ar balto saikni, ja vaicājumu veicošajai iestādei saskaņā ar Savienības vai valsts tiesību aktiem ir piekļuve saistītajiem datiem.

3. Ja ir izveidota balta saikne starp datiem no IIS, VIS, *ETIAS*, *Eurodac* vai *ECRIS-TCN*, *CIR* glabāto personas datni atjaunina saskaņā ar 19. panta 2. punktu.

4. Neskarot Regulās (ES) 2018/1860, (ES) 2018/1861 un (ES) 2018/1862 minētos noteikumus par brīdinājumu apstrādi *SIS* un neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību un sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta valsts veikta izmeklēšana, gadījumos, kad pēc atšķirīgu identitāšu manuālas verifikācijas ir izveidota balta saikne, par atšķirīgu identitāšu manuālu verifikāciju atbildīgā iestāde informē attiecīgo personu par līdzīgu vai atšķirīgu identitātes datu esamību un sniedz personai vienotu identifikācijas numuru, kā minēts šīs regulas 34. panta c) punktā, atsauci uz iestādi, kas atbild par atšķirīgu identitāšu manuālu verifikāciju, kā minēts šīs regulas 34. panta d) punktā, un saskaņā ar šīs regulas 49. pantu izveidotā tīmekļa portāla tīmekļa adresi.

5. Ja kādas dalībvalsts iestādes rīcībā ir pierādījumi, ka baltā saikne ir nepareizi reģistrēta *MID*, ka baltā saikne nav atjaunināta vai ka dati ir apstrādāti *MID* vai ES informācijas sistēmās, pārkāpjot šo regulu, tā pārbauda attiecīgos datus, kas glabājas *CIR* un *SIS*, un vajadzības gadījumā nekavējoties labo vai dzēš saikni no *MID*. Minētā dalībvalsts iestāde nekavējoties informē dalībvalsti, kas atbildīga par atšķirīgu identitāšu manuālu verifikāciju.

6. Par atšķirīgo identitāšu manuālu verifikāciju atbildīgā iestāde sniedz 4. punktā minēto informāciju rakstveidā standarta veidlapā. Šīs veidlapas saturu un izklāstu nosaka Komisija ar īstenošanas aktiem. Minētos īstenošanas aktus pieņem saskaņā ar 70. panta 2. punktā minēto pārbaudes procedūru.

34. pants

Identitātes apstiprinājuma datne

Identitātes apstiprinājuma datnē ir iekļauti šādi dati:

a) saiknes, kas minētas 30. līdz 33. pantā;

b) atsauce uz ES informācijas sistēmām, kurās ir saistītie dati;

c) vienots identifikācijas numurs, kas ļauj izgūt saistītos datus no atbilstošajām ES informācijas sistēmām;

d) iestāde, kas atbild par atšķirīgu identitāšu manuālu verifikāciju;

e) saiknes izveides vai atjaunināšanas datums.

35. pants

Datu saglabāšana vairāku identitāšu detektorā

Identitātes apstiprinājuma datnes un tajās esošus datus, tostarp saiknes, glabā *MID* tikai tik ilgi, kamēr saistītie dati tiek glabāti divās vai vairākās ES informācijas sistēmās. To dzēšanu no *MID* veic automatizēti.

36. pants

Reģistra ierakstu glabāšana

1. *eu-LISA* glabā reģistra ierakstus par visām *MID* veiktajām datu apstrādes darbībām. Minētie reģistra ieraksti ietver šādu informāciju:

a) dalībvalsts, kas uzsāk meklēšanu;

b) lietotāja piekļuves nolūks;

c) vaicājuma datums un laiks;

d) vaicājuma vai vaicājumu veikšanai izmantoto datu veids;

e) atsauce uz saistītajiem datiem;

f) identitātes apstiprinājuma datnes vēsture.

2. Katra dalībvalsts glabā reģistra ierakstus par vaicājumiem, ko veic to iestādes un minēto iestāžu darbinieki, kuri ir pienācīgi pilnvaroti izmantot *MID*. Katra Savienības aģentūra glabā reģistra ierakstus par vaicājumiem, ko veic tās darbinieki, kuri ir pienācīgi pilnvaroti.

3. Reģistra ierakstus, kas minēti 1. un 2. punktā, var izmantot tikai datu aizsardzības uzraudzībai, tostarp tam, lai pārbaudītu vaicājuma pieļaujamību un datu apstrādes likumīgumu, un datu drošības un integritātes nodrošināšanai. Minētos reģistra ierakstus aizsargā ar atbilstīgiem pasākumiem, lai tiem nepiekļūtu nepilnvarotas personas, un tos dzēš vienu gadu pēc to izveides. Tomēr, ja tie ir nepieciešami jau iesāktās uzraudzības procedūrās, tos dzēš pēc tam, kad uzraudzības procedūrām minētie reģistra ieraksti vairs nav vajadzīgi.

VI NODAĻA

Pasākumi sadarbspējas atbalstam

37. pants

Datu kvalitāte

1. Neskarot dalībvalstu pienākumus saistībā ar sistēmās ievadīto datu kvalitāti, *eu-LISA* izveido automatizētus datu kvalitātes kontroles mehānismus un procedūras attiecībā uz datiem, kas glabāti *SIS*, *Eurodac*, *ECRIS-TCN*, kopējā *BMS* un *CIR*.

2. *eu-LISA* īsteno mehānismus kopējā *BMS* precizitātes novērtēšanai, datu kvalitātes indikatorus un minimālos kvalitātes standartus datu glabāšanai *SIS*, *Eurodac*, *ECRIS-TCN*, kopējā *BMS* un *CIR*.

SIS, *Eurodac*, *ECRIS-TCN*, kopējā *BMS*, *CIR* un *MID* var ievadīt tikai tādus datus, kas atbilst minimālajiem kvalitātes standartiem.

3. *eu-LISA* regulāri sniedz dalībvalstīm ziņojumus par automatizētajiem datu kvalitātes kontroles mehānismiem un procedūrām un kopējiem datu kvalitātes indikatoriem. *eu-LISA* arī regulāri sniedz Komisijai ziņojumus par jautājumiem, ar ko tā saskārusies, un dalībvalstīm, kurus tie skar. *eu-LISA* minēto ziņojumu pēc pieprasījuma sniedz arī Eiropas Parlamentam un Padomei. Nevienā ziņojumā, kuru izstrādā saskaņā ar šo punktu, nedrīkst būt personas dati.

4. Īstenošanas aktos paredz sīki izstrādātus noteikumus – jo īpaši attiecībā uz biometriskajiem datiem – par automatizētajiem datu kvalitātes kontroles mehānismiem un procedūrām, kopējiem datu kvalitātes indikatoriem un minimālajiem kvalitātes standartiem datu glabāšanai *SIS*, *Eurodac*, *ECRIS-TCN*, kopējā *BMS* un *CIR*. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

5. Vienu gadu pēc automatizēto datu kvalitātes kontroles mehānismu un procedūru, kopējo datu kvalitātes indikatoru un datu minimālo kvalitātes standartu izveides un turpmāk ik gadu Komisija izvērtē datu kvalitātes īstenošanu dalībvalstīs un sniedz jebkādus nepieciešamos ieteikumus. Dalībvalstis iesniedz Komisijai rīcības plānu par to, kā novērst visus izvērtēšanas ziņojumā konstatētos trūkumus, un jo īpaši par datu kvalitātes problēmām, kas radušās no kļūdainiem datiem ES informācijas sistēmās. Dalībvalstis regulāri ziņo Komisijai par šā rīcības plāna īstenošanā panākto progresu tik ilgi, kamēr tas ir pilnībā īstenots.

Komisija izvērtēšanas ziņojumu nosūta Eiropas Parlamentam, Padomei, Eiropas Datu aizsardzības uzraudzītājam, Eiropas Datu aizsardzības kolēģijai un Eiropas Savienības Pamattiesību aģentūrai, kas izveidota ar Padomes Regulu (EK) Nr. 168/2007 ([37]).

38. pants

Vienotais ziņojuma formāts

1. Ar šo tiek izveidots vienotais ziņojuma formāts (*UMF*). Ar *UMF* nosaka standartus konkrētiem satura elementiem attiecībā uz pārrobežu informācijas apmaiņu starp informācijas sistēmām, iestādēm vai organizācijām tieslietu un iekšlietu jomā.

([37]) Padomes Regula (EK) Nr. 168/2007 (2007. gada 15. februāris), ar ko izveido Eiropas Savienības Pamattiesību aģentūru (OV L 53, 22.2.2007., 1. lpp.).

2. *UMF* standartu, ja tas ir iespējams, izmanto *Eurodac*, *ECRIS-TCN*, *ESP*, *CIR* un *MID* izstrādē, kā arī – vajadzības gadījumā – jaunu informācijas apmaiņas modeļu un informācijas sistēmu izstrādē, ko tieslietu un iekšlietu jomā veic *eu-LISA* vai jebkura cita Savienības aģentūra.

3. Komisija pieņem īstenošanas aktu, lai noteiktu un izstrādātu šā panta 1. punktā minēto *UMF* standartu. Minēto īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

39. pants

Centrālais ziņošanas un statistikas repozitorijs

1. Izveido centrālu ziņošanas un statistikas repozitoriju (*CRRS*), lai saskaņā ar attiecīgajiem tiesību instrumentiem, kas reglamentē *SIS*, *Eurodac* un *ECRIS-TCN*, atbalstītu minēto sistēmu mērķus un lai politikas, operatīvos un datu kvalitātes nolūkos nodrošinātu vairākas sistēmas aptverošus statistikas datus un analītiskus ziņojumus.

2. *eu-LISA* savos tehniskajos centros izveido, ievieš un mitina *CRRS*, kurā ietverti dati un statistika, kas minēti Regulas (ES) 2018/1862 74. pantā un Regulas (ES) 2019/816 32. pantā un kas ir loģiski nodalīti atbilstoši ES informācijas sistēmai. Iestādēm, kas minētas Regulas (ES) 2018/1862 74. pantā un Regulas (ES) 2019/816 32. pantā, piešķir piekļuvi *CRRS* tikai pārskatu un statistikas vajadzībām, izmantojot kontrolētu, drošu piekļuvi un īpašus lietotāju profilus.

3. *eu-LISA* padara datus anonīmus un reģistrē šādus anonimizētus datus centrālajā ziņošanas un statistikas repozitorijā (*CRRS*). Process, kura gaitā datus padara anonīmus, ir automatizēts.

CRRS ietvertie dati nedod iespēju identificēt privātpersonas.

4. *CRRS* veido:

a) datu anonimizēšanai nepieciešamie rīki;

b) centrāla infrastruktūra, kas sastāv no datu repozitorija, kurā ir anonīmi dati;

c) droša komunikāciju infrastruktūra, kuras mērķis ir savienot *CRRS* ar *SIS*, *Eurodac* un *ECRIS-TCN*, kā arī ar kopējā *BMS*, *CIR* un *MID* centrālajām infrastruktūrām.

5. Komisija pieņem deleģēto aktu saskaņā ar 69. pantu, paredzot sīki izstrādātus noteikumus par *CRRS* darbību, tostarp īpašus aizsardzības pasākumus personas datu apstrādei atbilstīgi šā panta 2. un 3. punktam un drošības noteikumus, kas piemērojami repozitorijam.

VII NODAĻA

Datu aizsardzība

40. pants

Datu pārzinis

1. Saistībā ar datu apstrādi kopējā *BMS* dalībvalstu iestādes, kas ir pārziņi attiecībā uz *Eurodac*, *SIS* un *ECRIS-TCN*, ir pārziņi arī saskaņā ar Regulas (ES) 2016/679 4. panta 7. punktu vai Direktīvas (ES) 2016/680 3. panta 8. punktu attiecībā uz biometriskajām veidnēm, kuras iegūtas no šīs regulas 13. pantā minētajiem datiem, ko tās ievada pamatā esošajās sistēmās, un minētās iestādes ir atbildīgas par biometrisko veidņu apstrādi kopējā *BMS*.

2. Saistībā ar datu apstrādi *CIR* dalībvalstu iestādes, kas attiecīgi ir pārziņi attiecībā uz *Eurodac* un *ECRIS-TCN*, ir pārziņi arī saskaņā ar Regulas (ES) 2016/679 4. panta 7) punktu vai Direktīvas (ES) 2016/680 3. panta 8. punktu attiecībā uz šīs regulas 18. pantā minētajiem datiem, kurus tās ievada pamatā esošajās sistēmās, un minētās iestādes ir atbildīgas par minēto personas datu apstrādi *CIR*.

3. Attiecībā uz datu apstrādi *MID*:

a) Eiropas Robežu un krasta apsardzes aģentūra ir datu pārzinis Regulas (ES) 2018/1725 3. panta 8) punkta nozīmē attiecībā uz personas datu apstrādi, ko veic *ETIAS* centrālā vienība;

b) dalībvalstu iestādes, kas papildina vai groza identitātes apstiprinājuma datnē ietvertos datus, ir pārziņi saskaņā ar Regulas (ES) 2016/679 4. panta 7) punktu vai Direktīvas (ES) 2016/680 3. panta 8) punktu, un minētās iestādes ir atbildīgas par personas datu apstrādi *MID*;

4. Datu aizsardzības uzraudzības nolūkā, tostarp nolūkā pārbaudīt vaicājuma pieļaujamību un datu apstrādes likumību, datu pārziņiem ir piekļuve 10., 16., 24. un 36. pantā minētajiem reģistra ierakstiem pašuzraudzības vajadzībām, kā minēts 44. pantā.

41. pants

Datu apstrādātājs

Attiecībā uz personas datu apstrādi kopējā *BMS*, *CIR* un *MID* *eu-LISA* ir datu apstrādātājs Regulas (ES) 2018/1725 3. panta 12. punkta a) apakšpunkta nozīmē.

42. pants

Apstrādes drošība

1. *eu-LISA*, *ETIAS* centrālā vienība, Eiropols un dalībvalstu iestādes nodrošina saskaņā ar šo regulu veiktās personu datu apstrādes drošību. *eu-LISA*, *ETIAS* centrālā vienība, Eiropols un dalībvalstu iestādes sadarbojas ar drošību saistītajos uzdevumos.

2. Neskarot Regulas (ES) 2018/1725 33. pantu, *eu-LISA* veic vajadzīgos pasākumus, lai nodrošinātu sadarbspējas komponentu un ar tiem saistītās komunikācijas infrastruktūras drošību.

3. Jo īpaši *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 nepiederošām personām piekļuvi datu apstrādes aprīkojumam un iekārtām;

c) novērstu datu neatļautu nolasīšanu, kopēšanu, grozīšanu vai datu nesēju izņemšanu;

d) novērstu datu nesankcionētu ievadīšanu, kā arī liegtu reģistrēto personas datu nesankcionētu apskati, grozīšanu vai dzēšanu;

e) novērstu datu nesankcionētu apstrādi, kā arī datu nesankcionētu kopēšanu, grozīšanu vai dzēšanu;

f) liegtu iespēju nepilnvarotām personām, kas izmanto datu pārraides ierīces, lietot automatizētas datu apstrādes sistēmas;

g) nodrošinātu, ka personām, kas ir pilnvarotas piekļūt sadarbspējas komponentiem, ir piekļuve tikai tiem datiem, uz kuriem attiecas viņu piekļuves tiesības, izmantojot tikai individuālas lietotāju identitātes un konfidenciālus piekļuves režīmus;

h) nodrošinātu to, ka var pārbaudīt un noteikt, kurām struktūrām personas datus var pārraidīt, izmantojot datu pārraides ierīces;

i) nodrošinātu iespēju pārbaudīt un noteikt, kādi dati ir apstrādāti sadarbspējas komponentos, kad, kas un kādam mērķim tos ir apstrādājis;

j) nodrošinātu, jo īpaši ar pienācīgu šifrēšanas paņēmienu palīdzību, ka laikā, kad personu datus pārraida uz sadarbspējas komponentiem vai no tiem, vai datu nesēju transportēšanas laikā tos nevar nesankcionēti nolasīt, kopēt, grozīt vai dzēst;

k) nodrošinātu, ka traucējuma gadījumā ir iespējams atjaunot uzstādīto sistēmu normālu darbību;

l) nodrošinātu uzticamību, garantējot, ka jebkuras sadarbspējas komponentu darbības kļūmes tiek pienācīgi darītas zināmas;

m) uzraudzītu šajā punktā minēto drošības pasākumu efektivitāti un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību ar mērķi nodrošināt atbilstību šai regulai un novērtēt šos drošības pasākumus, ņemot vērā jaunos tehnoloģiskos sasniegumus.

4. Dalībvalstis, Eiropols un *ETIAS* centrālā vienība pieņem 3. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar personas datu apstrādi, ko veic iestādes, kurām ir tiesības piekļūt jebkuram sadarbspējas komponentam.

43. pants

Drošības incidenti

1. Jebkuru notikumu, kas ietekmē vai var ietekmēt sadarbspējas komponentu drošību un var kaitēt tajos glabātajiem datiem vai izraisīt to zudumu, uzskata par drošības incidentu, jo īpaši, ja ir notikusi nesankcionēta piekļuve datiem vai ir apdraudēta vai varētu būt tikusi apdraudēta datu pieejamība, integritāte un konfidencialitāte.

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

3. Neskarot Regulas (ES) 2016/679 33. pantā, Direktīvas (ES) 2016/680 30. pantā vai abos paredzēto paziņošanu par personas datu aizsardzības pārkāpumu, dalībvalstis nekavējoties paziņo Komisijai, *eu-LISA*, kompetentajām uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītājam par visiem drošības incidentiem.

Neskarot Regulas (ES) 2018/1725 34. un 35. pantu un Regulas (ES) 2016/794 34. pantu, *ETIAS* centrālā vienība un Eiropols nekavējoties paziņo Komisijai, *eu-LISA* un Eiropas Datu aizsardzības uzraudzītājam par visiem drošības incidentiem.

Ja noticis drošības incidents saistībā ar sadarbspējas komponentu centrālo infrastruktūru, *eu-LISA* par to nekavējoties paziņo Komisijai un Eiropas Datu aizsardzības uzraudzītājam.

4. Informāciju par drošības incidentu, kam ir vai var būt ietekme uz sadarbspējas komponentu darbību vai uz datu pieejamību, integritāti un konfidencialitāti, nekavējoties sniedz dalībvalstīm, *ETIAS* centrālajai vienībai, un Eiropolam, un par to ziņo atbilstīgi incidentu pārvaldības plānam, ko nodrošina *eu-LISA*.

5. Attiecīgās dalībvalstis, *ETIAS* centrālā vienība, Eiropols un *eu-LISA* drošības incidenta gadījumā sadarbojas. Komisija ar īstenošanas aktiem nosaka šīs sadarbības procedūras kārtību. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

44. pants

Pašuzraudzība

Dalībvalstis un attiecīgās Savienības aģentūras nodrošina, ka katra iestāde, kurai ir tiesības piekļūt sadarbspējas komponentiem, veic vajadzīgos pasākumus, lai uzraudzītu savu atbilstību šai regulai, un vajadzības gadījumā sadarbojas ar uzraudzības iestādi.

Šīs regulas 40. pantā minētie datu pārziņi veic vajadzīgos pasākumus, lai uzraudzītu saskaņā ar šo regulu veiktās datu apstrādes atbilstību, tostarp bieži pārbaudot 10., 16., 24. un 36. pantā minētos reģistra ierakstus, un vajadzības gadījumā sadarbojas ar uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju.

45. pants

Sankcijas

Dalībvalstis nodrošina, ka par jebkādu datu nepareizu izmantošanu, datu apstrādi vai datu apmaiņu, kas ir pretrunā šai regulai, piemēro sankcijas saskaņā ar valsts tiesību aktiem. Paredzētās sankcijas ir efektīvas, samērīgas un atturošas.

46. pants

Atbildība

1. Neskarot tiesības uz kompensāciju no pārziņa vai apstrādātāja un pārziņa vai apstrādātāja atbildību saskaņā ar Regulu (ES) 2016/679, Direktīvu (ES) 2016/680 un Regulu (ES) 2018/1725:

a) jebkurai personai vai dalībvalstij, kurai ir nodarīts materiāls vai nemateriāls kaitējums tādas nelikumīgas personas datu apstrādes darbības vai jebkuras citas ar šo regulu nesaderīgas tādas rīcības rezultātā, kuru ir veikusi dalībvalsts, ir tiesības saņemt kompensāciju no minētās dalībvalsts;

b) jebkurai personai vai dalībvalstij, kam nodarīts materiāls vai nemateriāls kaitējums ar šo regulu nesaderīgas rīcības rezultātā, kuru veicis Eiropols, Eiropas Robežu un krasta apsardzes aģentūra vai *eu-LISA*, ir tiesības saņemt kompensāciju no minētās aģentūras.

Attiecīgo dalībvalsti, Eiropolu, Eiropas Robežu un krasta apsardzes aģentūru vai *eu-LISA* pilnībā vai daļēji atbrīvo no pirmajā daļā noteiktās atbildības, ja tie pierāda, ka nav atbildīgi par notikumu, kas ir izraisījis minēto kaitējumu.

2. Ja sakarā ar to, ka kāda dalībvalsts nav ievērojusi šajā regulā noteiktus pienākumus, ir nodarīts kaitējums sadarbspējas komponentiem, minētā dalībvalsts ir atbildīga par šādu kaitējumu, izņemot gadījumu, kad un ciktāl *eu-LISA* vai cita dalībvalsts, kurai ir jāievēro šī regula, nav veikusi saprātīgus pasākumus, lai kaitējumu novērstu vai mazinātu tā sekas.

3. Pret dalībvalsti vērstas prasības attiecībā uz kompensāciju par kaitējumu, kas ir minēts 1. un 2. punktā, reglamentē atbildētājas dalībvalsts tiesību akti. Pret pārzini vai *eu-LISA* vērstām kompensācijas prasībām par kaitējumu, kas ir minēts 1. un 2. punktā, piemēro Līgumos paredzētos nosacījumus.

47. pants

Tiesības uz informāciju

1. Iestāde, kas vāc personas datus, kuri glabājami kopējā *BMS*, *CIR* vai *MID*, sniedz personām, kuru dati tiek vākti, informāciju, kas ir jāsniedz saskaņā ar Regulas (ES) 2016/679 13. un 14. pantu, Direktīvas (ES) 2016/680 12. un 13. pantu un Regulas (ES) 2018/1725 15. un 16. pantu. Minētā iestāde sniedz informāciju brīdī, kad šādus datus ievāc.

2. Informāciju dara pieejamu skaidrā un vienkāršā valodā tādas valodas versijā, kuru attiecīgā persona saprot vai par kuru var pamatoti sagaidīt, ka tā to saprot. Tas attiecas arī uz vecumam atbilstošu informācijas sniegšanu datu subjektiem, kuri ir nepilngadīgie.

3. Personas datiem, ko reģistrē *ECRIS-TCN* un apstrādā šīs regulas nolūkā, piemēro noteikumus par tiesībām uz informāciju, kas paredzēti piemērojamos Savienības datu aizsardzības noteikumos.

48. pants

Tiesības piekļūt *MID* glabātajiem personas datiem, tos labot un dzēst un ierobežot to apstrādi

1. Lai īstenotu Regulas (ES) 2016/679 15. līdz 18. pantā, Regulas (ES) 2018/1725 17. līdz 20. pantā un Direktīvas (ES) 2016/680 14., 15. un 16. pantā noteiktās tiesības, ikvienai personai ir tiesības vērsties jebkuras dalībvalsts kompetentajā iestādē, kas izskata pieprasījumu un atbild uz to.

2. Dalībvalsts, kura izskata šādu pieprasījumu, atbild bez nepamatotas kavēšanās un jebkurā gadījumā ne vēlāk kā 45 dienu laikā pēc pieprasījuma saņemšanas. Vajadzības gadījumā minēto laikposmu var pagarināt vēl par 15 dienām, ņemot vērā pieprasījumu sarežģītību un skaitu. Dalībvalsts, kura izskata šādu pieprasījumu, informē datu subjektu par jebkuru šādu pagarinājumu un kavēšanās iemesliem 45 dienu laikā pēc pieprasījuma saņemšanas. Dalībvalstis var nolemt, ka atbildes sniedz centrālie biroji.

3. Ja personas datu labošanas vai dzēšanas pieprasījumu iesniedz citai dalībvalstij, nevis par atšķirīgu identitāšu manuālu verifikāciju atbildīgajai dalībvalstij, tās dalībvalsts iestādes, kurām pieprasījums iesniegts, septiņu dienu laikā sazinās ar tās dalībvalsts iestādēm, kas atbildīga par atšķirīgu identitāšu manuālu verifikāciju. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts bez nepamatotas kavēšanās un jebkurā gadījumā 30 dienu laikā pēc šādas sazināšanās pārbauda datu pareizību un datu apstrādes likumību. Vajadzības gadījumā minēto laikposmu var pagarināt vēl par 15 dienām, ņemot vērā pieprasījumu sarežģītību un skaitu. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts informē dalībvalsti, kura ar to sazinājusies, par jebkuru šādu pagarinājumu un par kavēšanās iemesliem. Dalībvalsts, kas ir sazinājusies ar tās dalībvalsts iestādi, kura atbildīga par atšķirīgu identitāšu manuālu verifikāciju, informē attiecīgo personu par turpmāko procedūru.

4. Ja personas datu labošanas vai dzēšanas pieprasījumu iesniedz dalībvalstij un ja par atšķirīgu identitāšu manuālu verifikāciju bija atbildīga *ETIAS* centrālā vienība, tās dalībvalsts iestādes, kurām pieprasījums iesniegts, septiņu dienu laikā sazinās ar *ETIAS* centrālo vienību un lūdz tai sniegt atzinumu. *ETIAS* centrālā vienība sniedz atzinumu bez nepamatotas kavēšanās un jebkurā gadījumā 30 dienu laikā pēc sazināšanās ar to. Vajadzības gadījumā minēto laikposmu var pagarināt vēl par 15 dienām, ņemot vērā pieprasījumu sarežģītību un skaitu. Dalībvalsts, kura sazinājās ar *ETIAS* centrālo vienību, informē attiecīgo personu par turpmāko procedūru.

5. Ja pēc pārbaudes tiek konstatēts, ka *MID* glabātie dati ir neprecīzi vai ir reģistrēti nelikumīgi, tad par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts vai, ja par atšķirīgu identitāšu manuālu verifikāciju nebija atbildīga neviena dalībvalsts vai ja par atšķirīgu identitāšu manuālu verifikāciju bija atbildīga *ETIAS* centrālā vienība, dalībvalsts, kurai iesniegts pieprasījums, bez nepamatotas kavēšanās labo vai dzēš minētos datus. Attiecīgo personu rakstiski informē, ka tās dati ir laboti vai dzēsti.

6. Ja dalībvalsts ievieš grozījumus *MID* glabātajos datos to saglabāšanas periodā, attiecīgā dalībvalsts veic 27. pantā un – vajadzības gadījumā – 29. pantā paredzēto apstrādi, lai noteiktu, vai grozītie dati ir jāsaista. Ja apstrāde neuzrāda nevienu atbilstību, attiecīgā dalībvalsts dzēš datus no identitātes apstiprinājuma datnes. Ja automatizētā apstrāde uzrāda vienu vai vairākas atbilstības, attiecīgā dalībvalsts izveido vai atjaunina attiecīgo saikni saskaņā ar attiecīgajiem šīs regulas noteikumiem.

7. Ja par atšķirīgo identitāšu manuālu verifikāciju atbildīgā dalībvalsts vai – vajadzības gadījumā – dalībvalsts, kurai iesniegts pieprasījums, nepiekrīt tam, ka *MID* glabātie dati ir neprecīzi vai ir reģistrēti nelikumīgi, minētā dalībvalsts pieņem administratīvu lēmumu, kurā attiecīgajai personai nekavējoties rakstiski paskaidrots, kāpēc valsts atsakās labot vai dzēst datus, kas attiecas uz šo personu.

8. Ar 7. punktā minēto lēmumu attiecīgajai personai arī sniedz informāciju, kurā izskaidrota iespēja pārsūdzēt lēmumu, kas pieņemts saistībā ar pieprasījumu piekļūt personas datiem, tos labot, dzēst vai ierobežot to apstrādi, un – vajadzības gadījumā – informāciju par to, kā celt prasību vai iesniegt sūdzību kompetentajās iestādēs vai tiesās, kā arī informāciju par jebkādu palīdzību, tostarp uzraudzības iestāžu palīdzību.

9. Visos pieprasījumos piekļūt personas datiem, tos labot vai dzēst vai ierobežot to apstrādi ietver informāciju, kura vajadzīga, lai identificētu attiecīgo personu. Minēto informāciju izmanto vienīgi tam, lai varētu īstenot šajā pantā minētās tiesības, un pēc tam to nekavējoties dzēš.

10. Par atšķirīgu identitāšu manuālu verifikāciju atbildīgā dalībvalsts vai – vajadzības gadījumā – dalībvalsts, kurai iesniegts pieprasījums, rakstveidā glabā ierakstu, ka tika iesniegts pieprasījums piekļūt personas datiem, tos labot vai dzēst vai ierobežot to apstrādi, un to, kā šis pieprasījums tika izskatīts, un nekavējoties dara minēto ierakstu pieejamu uzraudzības iestādēm.

11. Šis pants neskar nekādus šajā pantā minēto tiesību ierobežojumus, kas paredzēti saskaņā ar Regulu (ES) 2016/679 un Direktīvu (ES) 2016/680.

49. pants

Tīmekļa portāls

1. Lai būtu vieglāk izmantot tiesības piekļūt personas datiem, tos labot vai dzēst vai ierobežot to apstrādi, izveido tīmekļa portālu.

2. Tīmekļa portālā ir informācija par 47. un 48. pantā minētajām tiesībām un procedūrām un lietotāja saskarne, kas personām, kuru datus apstrādā *MID* un kuras tika informētas par sarkanas saiknes esamību saskaņā ar 32. panta 4. punktu, sniedz iespēju saņemt par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes kontaktinformāciju.

3. Lai iegūtu par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes kontaktinformāciju, personai, kuru datus apstrādā *MID*, būtu jāievada 34. panta d) punktā minētā atsauce uz iestādi, kas atbild par atšķirīgu identitāšu manuālu verifikāciju. Tīmekļa portāls izmanto šo atsauci, lai izgūtu par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes kontaktinformāciju. Tīmekļa portālā ir iekļauta arī e-pasta ziņojuma veidne, kuras nolūks ir atvieglot portāla lietotāja un par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentās iestādes saziņu. Šādā e-pasta ziņojumā ietver lauku 34. panta c) punktā minētajam vienotajam identifikācijas numuram, lai par atšķirīgu identitāšu manuālu verifikāciju atbildīgās dalībvalsts kompetentā iestāde varētu identificēt attiecīgos datus.

4. Dalībvalstis nodrošina *eu-LISA* visu to iestāžu kontaktinformāciju, kuras ir kompetentas izskatīt jebkuru 47. un 48. pantā minēto pieprasījumu un atbildēt uz to, un regulāri pārbauda, vai minētā kontaktinformācija ir aktualizēta.

5. *eu-LISA* izstrādā tīmekļa portālu un nodrošina tā tehnisko pārvaldību.

6. Komisija pieņem deleģēto aktu saskaņā ar 69. pantu, paredzot sīki izstrādātus noteikumus par tīmekļa portāla darbību, tostarp lietotāja saskarni, valodām, kurās tīmekļa portāls ir pieejams un e-pasta ziņojuma veidni.

50. pants

Personas datu nodošana trešām valstīm, starptautiskām organizācijām un privātām struktūrām

Neskarot Regulas (EK) Nr. 767/2008 31. pantu, Regulas (ES) 2016/794 25. un 26. pantu, Regulas (ES) 2017/2226 41. pantu, Regulas (ES) 2018/1240 65. pantu un tādus vaicājumus Interpola datubāzēs, kas veikti, izmantojot *ESP* saskaņā ar šīs regulas 9. panta 5. punktu, un atbilst Regulas (ES) 2018/1725 V nodaļas noteikumiem un Regulas (ES) 2016/679 V nodaļas noteikumiem, personas datus, kuri tiek glabāti sadarbspējas komponentos vai kurus apstrādā vai kuriem piekļūst ar sadarbspējas komponentu palīdzību, nenosūta vai nedara pieejamus nevienai trešai valstij, starptautiskai organizācijai vai privātai struktūrai.

51. pants

Uzraudzība, ko veic uzraudzības iestādes

1. Katra dalībvalsts nodrošina, ka uzraudzības iestādes neatkarīgi uzrauga personas datu apstrādes, ko attiecīgā dalībvalsts veic atbilstīgi šai regulai, tostarp datu pārraidīšanas uz sadarbspējas komponentiem un no tiem, likumību.

2. Katra dalībvalsts nodrošina, ka tās normatīvo un administratīvo aktu noteikumi, kas ir pieņemti, ievērojot Direktīvu (ES) 2016/680, vajadzības gadījumā ir piemērojami arī attiecībā uz policijas iestāžu un izraudzīto iestāžu piekļuvi sadarbspējas komponentiem, tostarp attiecībā uz to personu tiesībām, kuru datiem šādā veidā tās piekļūst.

3. Uzraudzības iestādes nodrošina, ka vismaz reizi četros gados tiek veikta to personas datu apstrādes darbību revīzija, ko veikušas atbildīgās valsts iestādes šīs regulas nolūkos, saskaņā ar attiecīgiem starptautiskiem revīzijas standartiem.

Uzraudzības iestādes katru gadu publisko personas datu labošanas, dzēšanas vai apstrādes ierobežojumu pieprasījumu skaitu, informāciju par turpmāk veiktajām darbībām un pēc attiecīgo personu pieprasījuma veikto labojumu, dzēšanu un apstrādes ierobežojumu skaitu.

4. Dalībvalstis nodrošina uzraudzības iestādēm pietiekamus resursus un zinātību, lai tās veiktu ar šo regulu uzticētos uzdevumus.

5. Dalībvalstis sniedz jebkādu informāciju, ko ir pieprasījusi Regulas (ES) 2016/679 51. panta 1. punktā minētā uzraudzības iestāde, un jo īpaši tai sniedz informāciju par darbībām, kas ir veiktas saskaņā ar dalībvalstu pienākumiem, kas noteikti šajā regulā. Dalībvalstis nodrošina Regulas (ES) 2016/679 51. panta 1. punktā minētajām uzraudzības iestādēm piekļuvi saviem reģistra ierakstiem, kas minēti šīs regulas 10., 16., 24. un 36. pantā, saviem pamatojumiem, kas minēti šīs regulas 22. panta 2. punktā, un ļauj tām jebkurā laikā iekļūt visās savās sadarbspējas nolūkā izmantotajās telpās.

52. pants

Revīzijas, ko veic Eiropas Datu aizsardzības uzraudzītājs

Eiropas Datu aizsardzības uzraudzītājs nodrošina, ka vismaz reizi četros gados tiek veikta *eu-LISA*, *ETIAS* centrālās vienības un Eiropola šīs regulas nolūkos veikto personas datu apstrādes darbību revīzija saskaņā ar attiecīgiem starptautiskiem revīzijas standartiem. Ziņojumu par minēto revīziju nosūta Eiropas Parlamentam, Padomei, *eu-LISA*, Komisijai, dalībvalstīm un attiecīgajai Savienības aģentūrai. Pirms ziņojumu pieņemšanas *eu-LISA*, *ETIAS* centrālajai vienībai un Eiropolam dod iespēju izteikt savus apsvērumus.

eu-LISA, *ETIAS* centrālā vienība un Eiropols sniedz Eiropas Datu aizsardzības uzraudzītājam tā pieprasīto informāciju, piešķir Eiropas Datu aizsardzības uzraudzītājam piekļuvi visiem dokumentiem, ko tas pieprasa, un saviem reģistra ierakstiem, kas ir minēti 10., 16., 24. un 36. pantā, un ļauj Eiropas Datu aizsardzības uzraudzītājam jebkurā laikā iekļūt visās to telpās.

53. pants

Uzraudzības iestāžu un Eiropas Datu aizsardzības uzraudzītāja sadarbība

1. Uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs, katrs rīkojoties savas attiecīgās kompetences robežās, aktīvi sadarbojas, ievērojot savus attiecīgos pienākumus, un nodrošina koordinētu sadarbspējas komponentu izmantošanas un šīs regulas noteikumu piemērošanas uzraudzību, jo īpaši tad, ja Eiropas Datu aizsardzības uzraudzītājs vai uzraudzības iestāde konstatē nozīmīgas neatbilstības Eiropas Savienības dalībvalstu praksē vai atklāj, iespējams, nelikumīgu nosūtīšanu, kas veikta, izmantojot sadarbspējas komponentu sakaru kanālus.

2. Gadījumos, kas minēti šā panta 1. punktā, nodrošina koordinētu uzraudzību saskaņā ar Regulas (ES) 2018/1725 62. pantu.

3. Eiropas Datu aizsardzības kolēģija Eiropas Parlamentam, Padomei, Komisijai, Eiropolam, Eiropas Robežu un krasta apsardzes aģentūrai un *eu-LISA* līdz 2021. gada 12. jūnijam un reizi divos gados pēc tam nosūta kopīgu ziņojumu par savu darbību saskaņā ar šo pantu. Minētajā ziņojumā iekļauj nodaļu par katru dalībvalsti, ko sagatavo attiecīgās dalībvalsts uzraudzības iestāde.

VIII NODAĻA

Pienākumi

54. pants

***eu-LISA* pienākumi plānošanas un izstrādes posmā**

1. *eu-LISA* nodrošina to, ka sadarbspējas komponentu centrālās infrastruktūras ekspluatē saskaņā ar šo regulu.

2. *eu-LISA* savos tehniskajos centros mitina sadarbspējas komponentus un nodrošina šajā regulā noteiktās funkcijas saskaņā ar 55. panta 1. punktā minētajiem drošības, pieejamības, kvalitātes un veiktspējas nosacījumiem.

3. *eu-LISA* ir atbildīga par sadarbspējas komponentu izstrādi un par jebkādiem pielāgojumiem, kas vajadzīgi, lai izveidotu sadarbspēju starp IIS, VIS, *ETIAS*, *SIS*, *Eurodac* un *ECRIS-TCN* centrālajām sistēmām, kā arī *ESP*, kopējo *BMS*, *CIR*, *MID* un *CRRS*.

Neskarot 62. pantu, *eu-LISA* nav piekļuves nekādiem personas datiem, kurus apstrādā, izmantojot *ESP*, kopējo *BMS*, *CIR* vai *MID*.

eu-LISA nosaka plānojumu sadarbspējas komponentu, tostarp to komunikācijas infrastruktūras un tehnisko specifikāciju, fiziskajai arhitektūrai, kā arī to attīstību attiecībā uz centrālo infrastruktūru un drošu komunikācijas infrastruktūru; minēto plānojumu pieņem valde, ņemot vērā Komisijas labvēlīgu atzinumu. *eu-LISA* arī ievieš visus nepieciešamos pielāgojumus *SIS*, *Eurodac* vai *ECRIS-TCN*, kuri izriet no sadarbspējas izveides un ir paredzēti šajā regulā.

eu-LISA izstrādā un ievieš sadarbspējas komponentus cik vien drīz iespējams pēc šīs regulas stāšanās spēkā un pēc tam, kad Komisija ir pieņēmusi 8. panta 2. punktā, 9. panta 7. punktā, 28. panta 5. un 7. punktā, 37. panta 4. punktā, 38. panta 3. punktā, 39. panta 5. punktā, 43. panta 5. punktā un 74. panta 10. punktā paredzētos pasākumus.

Izstrāde sastāv no tehnisko specifikāciju izstrādes un ieviešanas, testēšanas un projekta vispārējās vadības un koordinācijas.

4. Plānošanas un izstrādes posmā izveido Programmu vadības valdi, kurā ietilpst ne vairāk kā 10 locekļi. Tās sastāvā ir septiņi locekļi, kurus ieceļ *eu-LISA* valde no savu locekļu vai aizstājēju vidus, 71. pantā minētās padomdevēju grupas sadarbspējas jautājumos priekšsēdētājs, viens loceklis, kas pārstāv *eu-LISA* un ko iecēlis tās izpilddirektors, un viens Komisijas iecelts loceklis. *eu-LISA* valdes ieceltos locekļus ievēlē tikai no tām dalībvalstīm, kurām saskaņā ar Savienības tiesību aktiem ir pilnībā saistoši tiesību instrumenti, ar ko reglamentē visu ES informācijas sistēmu izstrādi, izveidi, darbību un izmantošanu, un kuras piedalīsies sadarbspējas komponentos.

5. Programmu vadības valde tiekas regulāri un vismaz trīs reizes ceturksnī. Tā nodrošina sadarbspējas komponentu plānošanas un izstrādes posma pienācīgu pārvaldību.

Programmu vadības valde katru mēnesi *eu-LISA* valdei iesniedz rakstiskus ziņojumus par projekta progresu. Programmu vadības valdei nav lēmumu pieņemšanas pilnvaru, nedz arī pilnvaru pārstāvēt *eu-LISA* valdes locekļus.

6. *eu-LISA* valde nosaka Programmu vadības valdes reglamentu, kurā jo īpaši iekļauj noteikumus par:

a) priekšsēdētāju;

b) sanāksmju vietām;

c) sanāksmju sagatavošanu;

d) ekspertu pielaidi sanāksmēm;

e) komunikācijas plāniem, kas nodrošina, ka klāt neesošie valdes locekļi tiek pilnībā informēti.

Priekšsēdētāja vietu ieņem dalībvalsts, kurai saskaņā ar Savienības tiesību aktiem ir pilnībā saistoši tiesību instrumenti, ar ko reglamentē visu ES informācijas sistēmu izstrādi, izveidi, darbību un izmantošanu, un kas piedalīsies sadarbspējas komponentos.

Visus ceļošanas un uzturēšanās izdevumus, kas rodas Programmu vadības valdes locekļiem, sedz *eu-LISA*, un *eu-LISA* reglamenta 10. pantu piemēro mutatis mutandis. *eu-LISA* Programmu vadības valdei nodrošina sekretariātu.

Šīs regulas 71. pantā minētā padomdevēju grupa sadarbspējas jautājumos regulāri tiekas līdz sadarbspējas komponentu darbības uzsākšanai. Pēc katras sanāksmes tā ziņo Programmu vadības valdei. Tā nodrošina tehnisko zinātību, lai sniegtu atbalstu Programmu vadības valdes uzdevumu veikšanā, un seko līdzi dalībvalstu gatavības situācijai.

55. pants

eu-LISA pienākumi pēc darbības uzsākšanas

1. Pēc katra sadarbspējas komponenta darbības uzsākšanas *eu-LISA* ir atbildīga par sadarbspējas komponentu centrālās infrastruktūras tehnisko pārvaldību, tostarp par to uzturēšanu un tehnoloģisko attīstību. Sadarbībā ar dalībvalstīm tā nodrošina, ka tiek izmantotas labākās pieejamās tehnoloģijas, pamatojoties uz izmaksu lietderīguma analīzi. *eu-LISA* ir atbildīga arī par 6., 12., 17., 25. un 39. pantā minētās komunikāciju infrastruktūras tehnisko pārvaldību.

Sadarbspējas komponentu tehniskā pārvaldība ir visi tie uzdevumi un tehniskie risinājumi, kuri vajadzīgi, lai 24 stundas diennaktī 7 dienas nedēļā nodrošinātu sadarbspējas komponentu darbību un nepārtrauktus pakalpojumus dalībvalstīm un Savienības aģentūrām saskaņā ar šo regulu. Tā ietver uzturēšanas darbus un tehnisko izstrādi, kas vajadzīga, lai nodrošinātu, ka komponentu darbības tehniskā kvalitāte ir apmierinošā līmenī, jo īpaši attiecībā uz reakcijas laiku, kurš vajadzīgs, lai sazinātos ar centrālajām infrastruktūrām saskaņā ar tehniskajām specifikācijām.

Visus sadarbspējas komponentus izstrādā un pārvalda tā, lai nodrošinātu ātru, raitu, efektīvu un kontrolētu piekļuvi, komponentu un *MID*, kopējā *BMS* un *CIR* glabāto datu pilnīgu un nepārtrauktu pieejamību un reakcijas laiku saskaņā ar dalībvalstu iestāžu un Savienības aģentūru funkcionālajām vajadzībām.

2. Neskarot 17. pantu Eiropas Savienības Civildienesta noteikumos, *eu-LISA* piemēro pienācīgus noteikumus par dienesta noslēpumu vai citas līdzvērtīgas konfidencialitātes prasības visiem saviem darbiniekiem, kuriem jāstrādā ar sadarbspējas komponentos glabātiem datiem. Šis pienākums ir spēkā arī tad, kad šie darbinieki vairs nav attiecīgajā amatā vai darbā, vai pēc tam, kad ir izbeigta to darbība.

Neskarot 62. pantu, *eu-LISA* nav piekļuves nekādiem personas datiem, kurus apstrādā, izmantojot *ESP*, kopējo *BMS*, *CIR* vai *MID*.

3. *eu-LISA* izstrādā un uztur mehānismu un procedūras kopējā *BMS* un *CIR* glabāto datu kvalitātes pārbaudēm saskaņā ar 37. pantu.

4. *eu-LISA* arī veic uzdevumus, kas saistīti ar apmācības sniegšanu par sadarbspējas komponentu tehnisko izmantošanu.

56. pants

Dalībvalstu pienākumi

1. Katra dalībvalsts ir atbildīga par:

a) savienošanu ar *ESP* un *CIR* komunikācijas infrastruktūru;

b) esošo valsts sistēmu un infrastruktūru integrāciju ar *ESP*, *CIR* un *MID*;

c) savas esošās valsts infrastruktūras organizāciju, pārvaldību, darbību un uzturēšanu un tās savienošanu ar sadarbspējas komponentiem;

d) kompetento valsts iestāžu darbinieku, kuriem pienācīgā kārtā izsniegta atļauja, piekļuves *ESP*, *CIR* un *MID* pārvaldību un organizēšanu saskaņā ar šo regulu un minēto darbinieku un viņu profilu saraksta izveidi un regulāru atjaunināšanu;

e) 20. panta 5. un 6. punktā minēto leģislatīvo pasākumu pieņemšanu, lai identifikācijas nolūkos nodrošinātu piekļuvi *CIR*;

f) atšķirīgu identitāšu manuālu verifikāciju, kas minēta 29. pantā;

g) atbilstību saskaņā ar Savienības tiesību aktiem noteiktajām datu kvalitātes prasībām;

h) atbilstību katras ES informācijas sistēmas noteikumiem par personas datu drošību un integritāti;

i) visu to trūkumu novēršanu, kuri konstatēti Komisijas izvērtēšanas ziņojumā attiecībā uz datu kvalitāti, kurš minēts 37. panta 5. punktā.

2. Katra dalībvalsts savieno savas izraudzītās iestādes ar *CIR*.

57. pants

Eiropola pienākumi

1. Eiropols nodrošina to Eiropola datu vaicājumu apstrādi, kurus veic *ESP*. Eiropols atbilstīgi pielāgo sava projekta *Querying Europol Systems* ("Vaicājumu veikšana Eiropola sistēmās") (*QUEST*) saskarni pamataizsardzības līmeņa (*BPL*) datiem.

2. Eiropols ir atbildīgs par savu pienācīgi pilnvaroto darbinieku pārvaldību un organizēšanu, lai saskaņā ar šo regulu attiecīgi izmantotu *ESP* un *CIR* un nodrošinātu piekļuvi tiem, kā arī par minēto darbinieku un viņu profilu saraksta izveidi un regulāru atjaunināšanu.

58. pants

***ETIAS* centrālās vienības pienākumi**

ETIAS centrālā vienība ir atbildīga par to, lai:

a) veiktu atšķirīgu identitāšu manuālo verifikāciju saskaņā ar 29. pantu;

b) veiktu 65. pantā minēto vairāku identitāšu konstatēšanu starp datiem, kas glabāti IIS, VIS, *Eurodac* un *SIS*.

IX NODAĻA

Grozījumi citos Savienības instrumentos

59. pants

Grozījumi Regulā (ES) 2018/1726

Regulu (ES) 2018/1726 groza šādi:

1) regulas 12. pantu aizstāj ar šādu:

"*12. pants*

Datu kvalitāte

1. Neskarot dalībvalstu pienākumus attiecībā uz datiem, kas ievadīti sistēmās, kuru darbības pārvaldība ir aģentūras atbildībā, visām sistēmām, kuru darbības pārvaldība ir aģentūras atbildībā, aģentūra, cieši iesaistot padomdevēju grupas, iedibina automatizētus datu kvalitātes kontroles mehānismus un procedūras, vienotus datu kvalitātes rādītājus un minimālos datu glabāšanas kvalitātes standartus saskaņā ar attiecīgajiem noteikumiem, kas izklāstīti tiesību instrumentos, kuri reglamentē minētās informācijas sistēmas, un Eiropas Parlamenta un Padomes Regulu (ES) 2019/817 (*) un (ES) 2019/818 (**) 37. pantā.

2. Aģentūra saskaņā ar Regulu (ES) 2019/817 un (ES) 2019/818 39. pantu izveido centrālu ziņošanas un statistikas repozitoriju, kurā ir tikai anonimizēti dati, ievērojot konkrētus to tiesību instrumentu noteikumus, kas reglamentē aģentūras pārvaldīto lielapjoma IT sistēmu izstrādi, izveidi, darbību un izmantošanu.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/817 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai robežu un vīzu jomā un groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 767/2008, (ES) 2016/399, (ES) 2017/2226, (ES) 2018/1240, (ES) 2018/1726 un (ES) 2018/1861 un Padomes Lēmumus 2004/512/EK un 2008/633/TI (OV L 135, 22.5.2019., 27. lpp.).

(**) Eiropas Parlamenta un Padomes Regula (ES) 2019/818 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai policijas un tiesu iestāžu sadarbības, patvēruma un migrācijas jomā un groza Regulas (ES) 2018/1726, (ES) 2018/1862 un (ES) 2019/816 (OV L 135, 22.5.2019., 85. lpp.).";

2) regulas 19. panta 1. punktu groza šādi:

a) iekļauj šādu apakšpunktu:

"eea) pieņem ziņojumus par stāvokli sadarbspējas komponentu izstrādē saskaņā ar Regulas (ES) 2019/817 78. panta 2. punktu un Regulas (ES) 2019/818 74. panta 2. punktu.";

b) punkta ff) apakšpunktu aizstāj ar šādu:

"ff) pieņem ziņojumus par *SIS* tehnisko darbību saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1861 (*) 60. panta 7. punktu un Eiropas Parlamenta un Padomes Regulas (ES) 2018/1862 (**) 74. panta 8. punktu, par VIS tehnisko darbību saskaņā ar Regulas (EK) Nr. 767/2008 50. panta 3. punktu un Lēmuma 2008/633/TI 17. panta 3. punktu, par IIS tehnisko darbību saskaņā ar Regulas (ES) 2017/2226 72. panta 4. punktu, par *ETIAS* tehnisko darbību saskaņā ar Regulas (ES) 2018/1240 92. panta 4. punktu, par *ECRIS-TCN* tehnisko darbību un ECRIS ieteicamo īstenošanu saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/816 (***) 36. panta 8. punktu un par sadarbspējas komponentu tehnisko darbību saskaņā ar Regulas (ES) 2019/817 78. panta 3. punktu un Regulas (ES) 2019/818 74. panta 3. punktu;

(*) Eiropas Parlamenta un Padomes Regula (ES) 2018/1861 (2018. gada 28. novembris) 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 312, 7.12.2018., 14. lpp.).

(**) Eiropas Parlamenta un Padomes Regula (ES) 2018/1862 (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 (OV L 312, 7.12.2018., 56. lpp.).

(***) Eiropas Parlamenta un Padomes Regula (ES) 2019/816 (2019. gada 17. aprīlis), ar ko Eiropas Sodāmības reģistru informācijas sistēmas papildināšanai un atbalstam izveido centralizētu sistēmu (*ECRIS-TCN*) tādu dalībvalstu identificēšanai, kurām ir informācija par notiesājošiem spriedumiem par trešo valstu valstspiederīgajiem un bezvalstniekiem, un ar ko groza Regulu (ES) 2018/1726 (OV L 135, 22.5.2019., 1. lpp.).";

c) punkta hh) apakšpunktu aizstāj ar šādu:

"hh) pieņem oficiālus komentārus par Eiropas Datu aizsardzības uzraudzītāja ziņojumiem par revīzijām saskaņā ar Regulas (ES) 2018/1861 56. panta 2. punktu, Regulas (EK) Nr. 767/2008 42. panta 2. punktu, Regulas (ES) Nr. 603/2013 31. panta 2. punktu, Regulas (ES) 2017/2226 56. panta 2. punktu, Regulas (ES) 2018/1240 67. pantu, Regulas (ES) 2019/816 29. panta 2. punktu un Regulu (ES) 2019/817 un (ES) 2019/818 52. pantu un nodrošina atbilstošus pēcpasākumus pēc šīm revīzijām;";

d) panta mm) apakšpunktu aizstāj ar šādu:

"mm) nodrošina, ka ik gadu publicē tādu kompetento iestāžu sarakstu, kas ir pilnvarotas veikt *SIS* iekļauto datu tiešu meklēšanu saskaņā ar Regulas (ES) 2018/1861 41. panta 8. punktu un Regulas (ES) 2018/1862 56. panta 7. punktu, kā arī *SIS* valstu sistēmu biroju (N.*SIS* biroji) un *SIRENE* biroju sarakstu, kā minēts attiecīgi Regulas (ES) 2018/1861 7. panta 3. punktā un Regulas (ES) 2018/1862 7. panta 3. punktā, kā arī kompetento iestāžu sarakstu saskaņā ar Regulas (ES) 2017/2226 65. panta 2. punktu, kompetento iestāžu sarakstu saskaņā ar Regulas (ES) 2018/1240 87. panta 2. punktu, centrālo iestāžu sarakstu saskaņā ar Regulas (ES) 2019/816 34. panta 2. punktu un iestāžu sarakstu saskaņā ar Regulas (ES) 2019/817 71. panta 1. punktu un Regulas (ES) 2019/818 67. panta 1. punktu;";

3) regulas 22. panta 4. punktu aizstāj ar šādu:

"4. Eiropols un *Eurojust* drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par *SIS* II saistībā ar Lēmuma 2007/533/TI piemērošanu.

Eiropas Robežu un krasta apsardzes aģentūra drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par *SIS* saistībā ar Regulas (ES) 2016/1624 piemērošanu.

Eiropols drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par VIS saistībā ar Lēmuma 2008/633/TI piemērošanu vai jautājums par *Eurodac* saistībā ar Regulas (ES) Nr. 603/2013 piemērošanu.

Eiropols drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par IIS saistībā ar Regulas (ES) 2017/2226 piemērošanu vai ja darba kārtībā ir jautājums par *ETIAS* saistībā ar Regulas (ES) 2018/1240 piemērošanu.

Eiropas Robežu un krasta apsardzes aģentūra arī drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par *ETIAS* saistībā ar Regulas (ES) 2018/1240 piemērošanu.

Eiropols, *Eurojust* un Eiropas Prokuratūra arī drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par Regulu (ES) 2019/816.

Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra arī drīkst piedalīties valdes sanāksmēs novērotāja statusā, ja darba kārtībā ir jautājums par Regulām (ES) 2019/817 un (ES) 2019/818.

Valde uz savām sanāksmēm novērotāja statusā var uzaicināt jebkuru citu personu, kuras viedoklis to varētu interesēt.";

4) regulas 24. panta 3. punkta p) apakšpunktu aizstāj ar šādu:

"p) to, lai, neskarot Civildienesta noteikumu 17. pantu, tiktu noteiktas konfidencialitātes prasības ar mērķi panākt atbilstību Regulas (EK) Nr. 1987/2006 17. pantam, Lēmuma 2007/533/TI 17. pantam, Regulas (EK) Nr. 767/2008 26. panta 9. punktam, Regulas (ES) Nr. 603/2013 4. panta 4. punktam, Regulas (ES) 2017/2226 37. panta 4. punktam, Regulas (ES) 2018/1240 74. panta 2. punktam, Regulas (ES) 2019/816 11. panta 16. punktam un Regulu (ES) 2019/817 un (ES) 2019/818 55. panta 2. punktam;";

5) regulas 27. pantu groza šādi:

a) panta 1. punktā iekļauj šādu apakšpunktu:

"da) padomdevēju grupa sadarbspējas jautājumos;";

b) panta 3. punktu aizstāj ar šādu:

"3. Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra var iecelt katrs savu pārstāvi *SIS* II padomdevēju grupā.

Eiropols var iecelt vienu pārstāvi arī VIS un *Eurodac*, un IIS-*ETIAS* padomdevēju grupās.

Eiropas Robežu un krasta apsardzes aģentūra arī var iecelt vienu pārstāvi IIS-*ETIAS* padomdevēju grupā.

Eurojust, Eiropols un Eiropas Prokuratūra var katrs iecelt vienu pārstāvi *ECRIS-TCN* padomdevēju grupā.

Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra var iecelt katrs savu pārstāvi padomdevēju grupā sadarbspējas jautājumos."

60. pants

Grozījumi Regulā (ES) 2018/1862

Regulu (ES) 2018/1862 groza šādi:

1) regulas 3. pantam pievieno šādus punktus:

"18) "*ESP*" ir Eiropas meklēšanas portāls, kas izveidots ar Eiropas Parlamenta un Padomes Regulas (ES) 2019/818 (*) 6. panta 1. punktu;

19) "kopējais *BMS*" ir kopējais biometrisko datu salīdzināšanas pakalpojums, kas izveidots ar Regulas (ES) 2019/818 12. panta 1. punktu;

20) "*CIR*" ir kopējais identitātes repozitorijs, kas izveidots ar Regulas (ES) 2019/818 17. panta 1. punktu;

21) "*MID*" ir vairāku identitāšu detektors, kas izveidots ar Regulas (ES) 2019/818 25. panta 1. punktu.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/818 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai policijas un tiesu iestāžu sadarbības, patvēruma un migrācijas jomā un groza Regulas (ES) 2018/1726, (ES) 2018/1862 un (ES) 2019/816 (OV L 135, 22.5.2019., 85. lpp.).";

2) regulas 4. pantu groza šādi:

a) panta 1. punkta b) un c) apakšpunktu aizstāj ar šādiem:

"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*;

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; un

d) droša komunikāciju infrastruktūra starp CS-*SIS* un *ESP*, kopējā *BMS* un *MID* centrālajām infrastruktūrām.";

b) pievieno šādus punktus:

"8. Neskarot šā panta 1. līdz 5. punktu, *SIS* datus par personām un personu apliecinošiem dokumentiem var arī meklēt, izmantojot *ESP*.

9. Neskarot šā panta 1.līdz 5. punktu, *SIS* datus par personām un personu apliecinošiem dokumentiem var arī nosūtīt, izmantojot drošo komunikāciju infrastruktūru, kas minēta 1. punkta d) apakšpunktā. Šī nosūtīšana nepārsniedz apjomu, kādā dati ir vajadzīgi Regulas (ES) 2019/818 nolūkiem.";

3) regulas 7. pantā iekļauj šādu punktu:

"2.a *SIRENE* biroji arī nodrošina atšķirīgu identitāšu manuālu verifikāciju saskaņā ar Regulas (ES) 2019/818 29. pantu. Ciktāl tas ir nepieciešams šā uzdevuma veikšanai, *SIRENE* birojiem ir piekļuve datiem, kurus glabā *CIR* un *MID*, Regulas (ES) 2019/818 21. un 26. pantā paredzētajos nolūkos.";

4) regulas 12. panta 1. punktam pievieno šādu daļu:

"Dalībvalstis nodrošina, ka katra piekļuve personas datiem, izmantojot *ESP*, arī tiek reģistrēta, lai varētu pārbaudīt, vai meklēšana bijusi likumīga, lai uzraudzītu datu apstrādes likumību, pašuzraudzības nolūkos un lai nodrošinātu datu integritāti un drošību.";

5) regulas 44. panta 1. punktam pievieno šādu apakšpunktu:

"f) pārbaudītu atšķirīgās identitātes un apkarotu identitātes viltošanu saskaņā ar Regulas (ES) 2019/818 V nodaļu.";

6) regulas 74. panta 7. punktu aizstāj ar šādu:

"7. Šīs regulas 15. panta 4. punkta un šā panta 3., 4. un 6. punkta nolūkos datus, kuri minēti 15. panta 4. punktā un šā panta 3. punktā un kuri neļauj identificēt personas, *eu-LISA* glabā centrālajā ziņošanas un statistikas repozitorijā, kas minēts Regulas (ES) 2019/818 39. pantā.

eu-LISA ļauj Komisijai un šā panta 6. punktā minētajām struktūrām iegūt pēc pasūtījuma sagatavotus ziņojumus un statistiku. Pēc pieprasījuma *eu-LISA* piešķir dalībvalstīm, Komisijai, Eiropolam un Eiropas Robežu un krasta apsardzes aģentūrai piekļuvi centrālajam ziņošanas un statistikas repozitorijam saskaņā ar Regulas (ES) 2019/818 39. pantu."

61. pants

Grozījumi Regulā (ES) 2019/816

Regulu (ES) 2019/816 groza šādi:

1) regulas 1. pantam pievieno šādu punktu:

"c) nosacījumus, saskaņā ar kuriem *ECRIS-TCN* ļauj atvieglot un palīdzēt veikt *ECRIS-TCN* reģistrēto personu pareizu identifikāciju saskaņā ar nosacījumiem un atbilstīgi nolūkiem, kas minēti Eiropas Parlamenta un Padomes Regulas (ES) 2019/818 (*) 20. pantā, ko panāk, glabājot *CIR* identitātes datus, ceļošanas dokumenta datus un biometriskos datus.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2019/818 (2019. gada 20. maijs), ar ko izveido satvaru ES informācijas sistēmu sadarbspējai policijas un tiesu iestāžu sadarbības, patvēruma un migrācijas jomā un groza Regulas (ES) 2018/1726, (ES) 2018/1862 un (ES) 2019/816 (OV L 135, 22.5.2019., 85. lpp.).";

2) regulas 2. pantu aizstāj ar šādu:

"*2. pants*

Darbības joma

Šo regulu piemēro tādu trešo valstu valstspiederīgo identitātes informācijas apstrādei, attiecībā uz kuriem dalībvalstīs ir pieņemti notiesājoši spriedumi, un mērķis ir identificēt dalībvalstis, kur šādi notiesājoši spriedumi ir pieņemti. Izņemot 5. panta 1. punkta b) apakšpunkta ii) punktu, šīs regulas noteikumus, kurus piemēro trešo valstu valstspiederīgajiem, piemēro arī tiem Savienības pilsoņiem, kuriem ir arī trešās valsts valstspiederība un attiecībā uz kuriem dalībvalstīs ir pieņemti notiesājoši spriedumi. Ar šo regulu arī atvieglo un palīdz veikt personu pareizu identifikāciju saskaņā ar šo regulu un Regulu (ES) 2019/818.";

3) regulas 3. pantu groza šādi:

a) panta 8) punktu svītro:

b) pievieno šādus punktus:

"19) "*CIR*" ir kopējais identitātes repozitorijs, kas izveidots ar Regulas (ES) 2019/818 17. panta 1. punktu;

20) "*ECRIS-TCN* dati" ir visi dati, kurus glabā centrālajā sistēmā un *CIR* saskaņā ar 5. pantu;

21) "*ESP*" ir Eiropas meklēšanas portāls, kas izveidots ar Regulas (ES) 2019/818 6. panta 1. punktu.";

4) regulas 4. panta 1. punktu groza šādi:

a) punkta a) apakšpunktu aizstāj ar šādu:

"a) centrālā sistēma;";

b) iekļauj šādu apakšpunktu:

"aa) *CIR*;";

c) pievieno šādu apakšpunktu:

"e) droša komunikāciju infrastruktūra starp centrālo sistēmu un *ESP* un *CIR* centrālajām infrastruktūrām;";

5) regulas 5. pantu groza šādi:

a) panta 1.punkta ievaddaļu aizstāj ar šādu:

"1. Katram notiesātajam trešās valsts valstspiederīgajam notiesāšanas dalībvalsts centrālā iestāde veic datu ierakstu *ECRIS-TCN*. Datu ierakstā iekļauj:";

b) iekļauj šādu punktu:

"1.a *CIR* ietilpst dati, kas minēti 1. punkta b) apakšpunktā, un šādi 1. punkta a) apakšpunktā minētie dati: uzvārds, uzvārds, vārdi, dzimšanas datums, dzimšanas vieta (pilsēta un valsts); valstspiederība vai valstspiederības, dzimums, attiecīgā gadījumā iepriekšējie vārdi, ja tādi ir pieejami – pseidonīmi vai pieņemtie vārdi, personas ceļošanas dokumentu veids un skaits, kā arī to izdevējiestādes nosaukums. *CIR* var ietvert 3. punktā minētos datus. Atlikušos *ECRIS-TCN* datus glabā centrālajā sistēmā.";

6) regulas 8. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Katru datu ierakstu centrālajā sistēmā un *CIR* glabā tik ilgi, kamēr sodāmības reģistros uzglabā datus, kas saistīti ar attiecīgo personu notiesājošiem spriedumiem.";

b) panta 2. punktu aizstāj ar šādu:

"2. Beidzoties 1. punktā minētajam saglabāšanas laikposmam, notiesāšanas dalībvalsts centrālā iestāde no centrālās sistēmas un *CIR* dzēš attiecīgo datu ierakstu, tostarp visus pirkstu nospiedumu datus un sejas attēlus. Dzēšana tiek veikts automātiski, ja iespējams, un jebkurā gadījumā ne vēlāk kā vienu mēnesi pēc tam, kad beidzies saglabāšanas laikposms.";

7) regulas 9. pantu groza šādi:

a) panta 1. punktā vārdu "*ECRIS-TCN*" aizstāj ar vārdiem "centrālajā sistēmā un *CIR*";

b) panta 2., 3. un 4. punktā vārdus "centrālā sistēma" attiecīgā locījumā aizstāj ar vārdiem "centrālā sistēma un *CIR*" attiecīgā locījumā;

8) regulas 10. panta 1. punkta j) apakšpunktu svītro;

9) regulas 12. panta 2. punktā vārdus "centrālajā sistēmā" aizstāj ar vārdiem "centrālajā sistēmā un *CIR*";

10) regulas 13. panta 2. punktā vārdus "centrālās sistēmas" aizstāj ar vārdiem "centrālās sistēmas, *CIR*";

11) regulas 23. panta 2. punktā vārdus "centrālajā sistēmā" aizstāj ar vārdiem "centrālajā sistēmā un *CIR*"";

12) regulas 24. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Centrālajā sistēmā un *CIR* ievadītos datus apstrādā tikai, lai identificētu dalībvalstis, kam ir sodāmības reģistra informācija par trešo valstu valstspiederīgajiem. *CIR* ievadītos datus apstrādā arī saskaņā ar Regulu (ES) 2019/818, lai saskaņā ar šo regulu atvieglotu *ECRIS-TCN* reģistrēto personu pareizu identifikāciju un palīdzētu to veikt.";

b) pievieno šādu punktu:

"3. Neskarot 2. punktu, piekļuvi, datu aplūkošanas nolūkos, kas tiek glabāti *CIR*, arī paredz to katras dalībvalsts iestāžu pienācīgi pilnvarotiem darbiniekiem un to Savienības aģentūru pienācīgi pilnvarotiem darbiniekiem, kuras ir kompetentas Regulas (ES) 2019/818 20. un 21. pantā noteiktajiem nolūkiem. Šāda piekļuve attiecas tikai uz datiem, kas vajadzīgi viņu uzdevumu pildīšanai minētajos nolūkos, un ir samērīga ar izvirzītajiem mērķiem.";

13) regulas 32. panta 2. punktu aizstāj ar šādu:

"2. Šā panta 1. punkta nolūkā *eu-LISA* glabā 1. punktā minētos datus centrālajā ziņošanas un statistikas repozitorijā, kas minēts Regulas (ES) 2019/818 39. pantā.";

14) regulas 33. panta 1. punktā vārdus "centrālās sistēmas" aizstāj ar vārdiem "centrālās sistēmas, *CIR* un";

15) regulas 41. panta 2. punktu aizstāj ar šādu:

"2. Attiecībā uz notiesājošiem spriedumiem, kas pieņemti pirms datu ievadīšanas sākuma datuma saskaņā ar 35. panta 1. punktu, centrālās iestādes izveido atsevišķus datu ierakstus centrālajā sistēmā un *CIR*, ņemot vērā, ka:

a) burtciparu datus centrālajā sistēmā un *CIR* ievada līdz 35. panta 2. punktā minētā laikposma beigām;

b) pirkstu nospiedumu datus centrālajā sistēmā un *CIR* ievada vēlākais divu gadu laikā pēc darbības sākuma saskaņā ar 35. panta 4. punktu."

X NODAĻA

Nobeiguma noteikumi

62. pants

Ziņošana un statistika

1. Dalībvalstu kompetento iestāžu, Komisijas un *eu-LISA* pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai tikai ziņošanas un statistikas nolūkos aplūkotu katra *ESP* lietotāja profila vaicājumu skaitu.

No datiem nav iespējams identificēt personas.

2. Dalībvalstu kompetento iestāžu, Komisijas un *eu-LISA* pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai tikai ziņošanas un statistikas nolūkos aplūkotu šādus datus, kas saistīti ar *CIR*:

a) vaicājumu skaits 20., 21. un 22. panta nolūkos;

b) personas valstspiederība, dzimums un dzimšanas gads;

c) ceļošanas dokumenta veids un izdevējas valsts trīs burtu kods;

d) to meklējumu skaits, kuri veikti, izmantojot un neizmantojot biometriskos datus.

No datiem nav iespējams identificēt personas.

3. Dalībvalstu kompetento iestāžu, Komisijas un *eu-LISA* pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai tikai ziņošanas un statistikas nolūkos aplūkotu šādus datus, kas saistīti ar *MID*:

a) to meklējumu skaits, kuri veikti, izmantojot un neizmantojot biometriskos datus;

b) katra veida saikņu skaits un tās ES informācijas sistēmas, kuras satur saistītos datus;

c) laikposms, kurā dzeltenā vai sarkanā saikne tika saglabāta sistēmā.

No datiem nav iespējams identificēt personas.

4. Eiropas Robežu un krasta apsardzes aģentūras pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai aplūkotu šā panta 1., 2. un 3. punktā minētos datus nolūkā veikt riska analīzi un neaizsargātības novērtējumus, kā minēts minētās Eiropas Parlamenta un Padomes Regulas (ES) 2016/1624 ([38]) 11. un 13. pantā.

5. Eiropola pienācīgi pilnvarotiem darbiniekiem ir piekļuve, lai aplūkotu šā panta 2. un 3. punktā minētos datus nolūkā veikt stratēģisko, tematisko un operatīvo analīzi, kā minēts Regulas (ES) 2016/794 18. panta 2. punkta b) un c) apakšpunktā.

6. Šā panta 1., 2. un 3. punkta nolūkā *eu-LISA* glabā minētajos punktos minētos datus *CRRS*. No *CRRS* iekļautajiem datiem nav iespējams identificēt personas, taču dati ļauj šā panta 1., 2. un 3. punktā uzskaitītajām iestādēm iegūt pielāgojamus pārskatus un statistiku, lai palielinātu robežpārbaužu efektivitāti, palīdzētu iestādēm apstrādāt vīzas pieteikumus un atbalstītu Savienībā uz faktiem pamatotas politikas veidošanu migrācijas un drošības jomā.

7. Komisija pēc pieprasījuma dara Eiropas Savienības Pamattiesību aģentūrai pieejamu attiecīgu informāciju, lai tā izvērtētu šīs regulas ietekmi uz pamattiesībām.

([38]) 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.).

63. pants

Pārejas periods Eiropas meklēšanas portāla izmantošanai

1. Divu gadu laikposmā no *ESP* darbības uzsākšanas nepiemēro 7. panta 2. un 4. punktā minētos pienākumus, un *ESP* izmantošana nav obligāta.

2. Komisija tiek pilnvarota pieņemt deleģēto aktu saskaņā ar 73. pantu, lai grozītu šo regulu, pagarinot šā panta 1. punktā minēto laikposmu vienu reizi uz laiku, kas nepārsniedz vienu gadu, ja *ESP* īstenošanas novērtējums liecina, ka šāds pagarinājums ir nepieciešams, īpaši ņemot vērā ietekmi, kādu *ESP* ieviešana radītu attiecībā uz robežpārbaužu organizāciju un ilgumu.

64. pants

Pārejas periods, ko piemēro noteikumiem par piekļuvi kopējam identitātes repozitorijam nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus

Šīs regulas 22. pantu piemēro no *CIR* darbības uzsākšanas dienas, kas minēta 68. panta 3. punktā.

65. pants

Pārejas periods vairāku identitāšu konstatēšanai

1. Viena gada laikposmā pēc tam, kad *eu-LISA* ir paziņojusi par 68. panta 4. punkta b) apakšpunktā minētā *MID* testa pabeigšanu, un pirms *MID* darbības uzsākšanas *ETIAS* centrālā vienība ir atbildīga par to, lai veiktu vairāku identitāšu konstatēšanu, izmantojot IIS, VIS, *Eurodac* un *SIS* glabātos datus. Vairāku identitāšu konstatēšanu veic, izmantojot vienīgi biometriskos datus.

2. Ja vaicājums uzrāda vienu vai vairākas atbilstības un identitātes dati saistītajās datnēs ir tādi paši vai līdzīgi, izveido baltu saikni saskaņā ar 33. pantu.

Ja vaicājums uzrāda vienu vai vairākas atbilstības un identitātes datus saistītajās datnēs nevar uzskatīt par līdzīgiem, izveido dzeltenu saikni saskaņā ar 30. pantu un piemēro 29. pantā minēto procedūru.

Ja tiek uzrādītas vairākas atbilstības, izveido saikni starp katru datu vienību, kas izraisa atbilstību.

3. Ja ir izveidota dzeltena saikne, *MID* piešķir *ETIAS* centrālajai vienībai piekļuvi dažādās ES informācijas sistēmās esošajiem identitātes datiem.

4. Ja ir izveidota saikne uz tādu brīdinājumu *SIS*, kas nav brīdinājums, kurš izveidots saskaņā ar Regulas (ES) 2018/1860 3. pantu, Regulas (ES) 2018/1861 24. un 25. pantu vai Regulas (ES) 2018/1862 38. pantu, tad *MID* piešķir brīdinājumu izveidojušās dalībvalsts *SIRENE* birojam piekļuvi dažādās informācijas sistēmās esošajiem identitātes datiem.

5. *ETIAS* centrālajai vienībai vai šā panta 4. punktā minētajos gadījumos tās dalībvalsts *SIRENE* birojam, kura izveidoja brīdinājumu, ir piekļuve identitātes apstiprinājuma datnē ietvertajiem datiem, un tie novērtē atšķirīgās identitātes un atjaunina saikni saskaņā ar 31., 32. un 33. pantu, un pievieno to identitātes apstiprinājuma datnei.

6. *ETIAS* centrālā vienība Komisijai saskaņā ar 67. panta 3. punktu paziņo tikai tad, kad visas dzeltenās saiknes ir manuāli verificētas un to status ir atjaunināts, pārveidojot tās par zaļajām, baltajām vai sarkanajām saiknēm.

7. Dalībvalstis vajadzības gadījumā palīdz *ETIAS* centrālajai vienībai veikt vairāku identitāšu konstatēšanu saskaņā ar šo pantu.

8. Komisija tiek pilnvarota pieņemt deleģēto aktu saskaņā ar 69. pantu, lai grozītu šo regulu, pagarinot šā panta 1. punktā minēto laikposmu par sešiem mēnešiem; šo pagarinājumu var atjaunot divas reizes, katru reizi uz sešiem mēnešiem. Šādu pagarinājumu piešķir tikai pēc vairāku identitāšu konstatēšanas pabeigšanas laika novērtējuma saskaņā ar šo pantu, ja tas liecina, ka vairāku identitāšu konstatēšanu nevar pabeigt pirms 1. punktā minētā laikposma vai jebkura pastāvoša pagarinājuma beigām no *ETIAS* centrālās vienības neatkarīgu apstākļu dēļ un korektīvus pasākumus nav iespējams piemērot. Novērtējumu veic ne vēlāk kā trīs mēnešus pirms šāda laikposma vai pastāvoša pagarinājuma beigām.

66. pants

Izmaksas

1. Izmaksas, kas rodas saistībā ar *ESP*, kopējā *BMS*, *CIR* un *MID* izveidi un darbību, sedz no Savienības vispārējā budžeta.

2. Izmaksas, kas rodas saistībā ar esošo valsts infrastruktūru integrāciju un šo infrastruktūru savienojumu ar valsts vienotajām saskarnēm, kā arī ar valsts vienoto saskarņu mitināšanu, sedz no Savienības vispārējā budžeta.

Netiek iekļautas šādas izmaksas:

a) dalībvalstu projektu vadības birojs (sanāksmes, komandējumi, biroji);

b) valstu IT sistēmu mitināšana (telpas, īstenošana, elektroenerģija, dzesēšana);

c) valstu IT sistēmu ekspluatācija (operatori un atbalsta līgumi);

d) valstu komunikācijas tīklu plānošana, izstrāde, ieviešana, ekspluatācija un uzturēšana.

3. Lai segtu šīs regulas īstenošanas izmaksas, kā paredzēts šā panta 1. un 2. punktā, neskarot šā mērķa turpmāku finansēšanu no citiem Eiropas Savienības vispārējā budžeta avotiem, tiek piesaistīti 32 077 000 EUR no Regulas (ES) Nr. 515/2014 5. panta 5. punkta b) apakšpunktā paredzētajiem 791 000 000 EUR.

4. No 3. punktā minētajiem finanšu līdzekļiem 22 861 000 EUR piešķir *eu-LISA*, 9 072 000 EUR piešķir Eiropolam un 144 000 EUR piešķir Eiropas Savienības Tiesībaizsardzības apmācības aģentūrai (*CEPOL*), lai palīdzētu šīm aģentūrām pildīt savus attiecīgos uzdevumus saskaņā ar šo regulu. Šo finansējumu īsteno ar netiešo pārvaldību.

5. Izmaksas, kas rodas izraudzītajām iestādēm, sedz attiecīgi izraudzītājas dalībvalstis. Izmaksas par katras izraudzītās iestādes savienojumu ar *CIR* sedz katra dalībvalsts.

Izmaksas, kas rodas Eiropolam, tostarp par savienojumu ar *CIR*, sedz Eiropols.

67. pants

Paziņojumi

1. Dalībvalstis paziņo *eu-LISA* par iestādēm, kuras minētas 7., 20., 21. un 26. pantā un kuras attiecīgi var izmantot *ESP*, *CIR* un *MID* vai kurām ir piekļuve tiem.

Minēto iestāžu konsolidētu sarakstu publicē Eiropas Savienības Oficiālajā Vēstnesī trīs mēnešu laikā no dienas, kad katrs sadarbspējas komponents ir uzsācis darbību saskaņā ar 68. pantu. Ja sarakstā ievieš grozījumus, *eu-LISA* reizi gadā publicē atjauninātu konsolidētu sarakstu.

2. *eu-LISA* paziņo Komisijai par 68. panta 1. punkta b) apakšpunktā, 2. punkta b) apakšpunktā, 3. punkta b) apakšpunktā, 4. punkta b) apakšpunktā, 5. punkta b) apakšpunktā un 6. punkta b) apakšpunktā minētā testa sekmīgu pabeigšanu.

3. *ETIAS* centrālā vienība paziņo Komisijai par 65. pantā paredzētā pārejas perioda sekmīgu pabeigšanu.

4. Komisija dara saskaņā ar 1. punktu paziņoto informāciju pieejamu dalībvalstīm un sabiedrībai, izmantojot publisku tīmekļa vietni, kura pastāvīgi tiek atjaunināta.

68. pants

Darbības sākums

1. Komisija ar īstenošanas aktu nosaka dienu, no kuras *ESP* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 8. panta 2. punktā, 9. panta 7. punktā un 43. panta 5. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *ESP* tests, ko *eu-LISA* ir veikusi, sadarbojoties ar dalībvalstu iestādēm un Savienības aģentūrām, kas var lietot *ESP*;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 8. panta 1. punktā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

ESP veic vaicājumus Interpola datubāzēs tikai tad, ja tehniskie pasākumi ļauj panākt atbilstību 9. panta 5. punktam. Ja nav iespējams nodrošināt atbilstību 9. panta 5. punktam, *ESP* neveic vaicājumus Interpola datubāzēs, bet tas neaizkavē *ESP* darbības sākumu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

2. Komisija ar īstenošanas aktu nosaka dienu, no kuras kopējais *BMS* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 13. panta 5. punktā un 43. panta 5. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs kopējā *BMS* tests, ko tā ir veikusi, sadarbojoties ar dalībvalstu iestādēm;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 13. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi Komisijai par minēto kārtību;

d) *eu-LISA* ir paziņojusi Komisijai par 5. punkta b) apakšpunktā minētā testa sekmīgu pabeigšanu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

3. Komisija ar īstenošanas aktu nosaka dienu, no kuras *CIR* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 43. panta 5. punktā un 74. panta 10. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *CIR* tests, ko tā ir veikusi, sadarbojoties ar dalībvalstu iestādēm;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 18. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

d) *eu-LISA* ir paziņojusi Komisijai par 5. punkta b) apakšpunktā minētā testa sekmīgu pabeigšanu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

4. Komisija ar īstenošanas aktu nosaka dienu, no kuras *MID* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 28. panta 5. un 7. punktā, 32. panta 5. punktā, 33. panta 6. punktā, 43. panta 5. punktā un 49. panta 6. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *MID* tests, ko tā ir veikusi, sadarbojoties ar dalībvalstu iestādēm un *ETIAS* centrālo vienību;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 34. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

d) *ETIAS* centrālā vienība ir paziņojusi Komisijai saskaņā ar 67. panta 3. punktu;

e) *eu-LISA* ir paziņojusi Komisijai par 1. punkta b) apakšpunktā, 2. punkta b) apakšpunktā, 3. punkta b) apakšpunktā un 5. punkta b) apakšpunktā minēto testu sekmīgu pabeigšanu.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

5. Komisija ar īstenošanas aktiem nosaka dienu, no kuras sāk izmantot automatizētos datu kvalitātes kontroles mehānismus un procedūras, kopējos datu kvalitātes indikatorus un datu kvalitātes minimālos standartus, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 37. panta 4. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs automatizēto datu kvalitātes kontroles mehānismu un procedūru, kopējo datu kvalitātes indikatoru un datu kvalitātes minimālo standartu tests, ko tā veikusi, sadarbojoties ar dalībvalstu iestādēm.

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

6. Komisija ar īstenošanas aktu nosaka dienu, no kuras *CRRS* sāk darbību, pēc tam, kad ir izpildīti šādi nosacījumi:

a) ir pieņemti 39. panta 5. punktā un 43. panta 5. punktā minētie pasākumi;

b) *eu-LISA* ir paziņojusi, ka ir sekmīgi pabeigts visaptverošs *CRRS* tests, ko tā veikusi, sadarbojoties ar dalībvalstu iestādēm;

c) *eu-LISA* ir validējusi tehnisko un juridisko kārtību 39. pantā minēto datu apkopošanai un pārsūtīšanai un paziņojusi to Komisijai;

Komisija pirmajā daļā minēto dienu nosaka tā, lai tā būtu 30 dienu laikā no īstenošanas akta pieņemšanas.

7. Komisija informē Eiropas Parlamentu un Padomi par saskaņā ar 1. punkta b) apakšpunktu, 2. punkta b) apakšpunktu, 3. punkta b) apakšpunktu, 4. punkta b) apakšpunktu, 5. punkta b) apakšpunktu un 6. punkta b) apakšpunktu veikto testu rezultātiem.

8. Dalībvalstis, *ETIAS* centrālā vienība un Eiropols sāk izmantot katru no sadarbspējas komponentiem no dienas, ko Komisija noteikusi attiecīgi saskaņā ar 1., 2., 3. un 4. punktu.

69. pants

Deleģēšanas īstenošana

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

2. Pilnvaras pieņemt 28. panta 5. punktā, 39. panta 5. punktā, 49. panta 6. punktā, 63. panta 2. punktā un 65. panta 8. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no 2019. gada 11. jūnija. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms piecu gadu laikposma beigām. Pilnvaru deleģēšana tiek automātiski pagarināta uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 28. panta 5. punktā, 39. panta 5. punktā, 49. panta 6. punktā, 63. panta 2. punktā un 65. panta 8. 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 28. panta 5. punktu, 39. panta 5. punktu, 49. panta 6. punktu, 63. panta 2. punktu un 65. panta 8. 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.

70. 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.

Ja komiteja atzinumu nesniedz, Komisija īstenošanas akta projektu nepieņem, un tiek piemērota Regulas (ES) Nr. 182/2011 5. panta 4. punkta trešā daļa.

71. pants

Padomdevēju grupa

eu-LISA izveido Sadarbspējas padomdevēju grupu. Sadarbspējas komponentu plānošanas un izstrādes posmā piemēro 54. panta 4., 5. un 6. punktu.

72. pants

Apmācība

Saskaņā ar Regulu (ES) 2018/1726 *eu-LISA* veic uzdevumus, kas saistīti ar apmācības sniegšanu par sadarbspējas komponentu tehnisko izmantošanu.

Dalībvalstu iestādes un Savienības aģentūras nodrošina saviem darbiniekiem, kas ir pilnvaroti apstrādāt datus, izmantojot sadarbspējas komponentus, atbilstīgas apmācības programmas par datu drošību, datu kvalitāti, datu aizsardzības noteikumiem, procedūrām, ko piemēro datu apstrādei, un pienākumiem sniegt informāciju saskaņā ar 32. panta 4. punktu, 33. panta 4. punktu un 47. pantu.

Attiecīgā gadījumā par minētajām tēmām organizē kopīgus mācību kursus Savienības līmenī, lai uzlabotu sadarbību un apmainītos ar paraugpraksi starp dalībvalstu iestāžu un Savienības aģentūru darbiniekiem, kas ir pilnvaroti apstrādāt datus, izmantojot sadarbspējas komponentus. Īpašu uzmanību pievērš vairāku identitāšu konstatēšanas procesam, tostarp atšķirīgu identitāšu manuālai verificēšanai un ar to saistītajai vajadzībai uzturēt atbilstošus pamattiesību aizsardzības pasākumus.

73. pants

Praktiskā rokasgrāmata

Komisija, cieši sadarbojoties ar dalībvalstīm, *eu-LISA* un citām attiecīgām Savienības aģentūrām, dara pieejamu praktisku rokasgrāmatu par sadarbspējas komponentu īstenošanu un pārvaldību. Praktiskā rokasgrāmata sniedz tehniskas un operatīvas norādes, ieteikumus un paraugpraksi. Komisija praktisko rokasgrāmatu pieņem ieteikuma veidā.

74. pants

Uzraudzība un izvērtēšana

1. *eu-LISA* nodrošina, ka ir ieviestas procedūras, lai uzraudzītu sadarbspējas komponentu izstrādi un to savienošanu ar valsts vienoto saskarni, ņemot vērā ar plānošanu un izmaksām saistītos mērķus, un lai uzraudzītu sadarbspējas komponentu darbību, ņemot vērā mērķus, kas saistīti ar pakalpojuma tehniskajiem rezultātiem, izmaksu lietderību, drošību un kvalitāti.

2. Līdz 2019. gada 12. decembrim un turpmāk ik pēc sešiem mēnešiem komponentu izstrādes posma laikā *eu-LISA* iesniedz ziņojumu Eiropas Parlamentam un Padomei par aktuālo situāciju saistībā ar sadarbspējas komponentu izstrādi, kā arī to savienojumu ar valsts vienoto saskarni. Tiklīdz izstrāde ir pabeigta, Eiropas Parlamentam un Padomei iesniedz ziņojumu, kurā sīki izskaidrots, kā tika sasniegti mērķi, jo īpaši saistībā ar plānošanu un izmaksām, kā arī pamatotas jebkādas atšķirības.

3. Četrus gadus pēc katra sadarbspējas komponenta darbības uzsākšanas saskaņā ar 68. pantu un turpmāk ik pēc četriem gadiem *eu-LISA* iesniedz Eiropas Parlamentam, Padomei un Komisijai ziņojumu par sadarbspējas komponentu tehnisko darbību, tostarp to drošību.

4. Turklāt vienu gadu pēc katra *eu-LISA* izstrādātā ziņojuma Komisija sagatavo sadarbspējas komponentu vispārēju izvērtējumu, kas ietver:

a) novērtējumu par šīs regulas piemērošanu;

b) salīdzinājumā ar šīs regulas mērķiem sasniegto rezultātu analīzi un tās ietekmi uz pamattiesībām, tostarp jo īpaši novērtējumu par sadarbspējas komponentu ietekmi uz tiesībām uz nediskriminēšanu;

c) novērtējumu par tīmekļa portāla darbību, tostarp tīmekļa portāla lietošanu raksturojošos rādītājus un izpildīto pieprasījumu skaitu;

d) novērtējumu par sadarbspējas komponentu pamatojuma turpmāku derīgumu;

e) novērtējumu par sadarbspējas komponentu drošību;

f) novērtējumu par to, kā identifikācijas nolūkā izmanto *CIR*;

g) novērtējumu par to, kā *CIR* izmanto nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus;

h) novērtējumu par jebkādām sekām, tostarp nesamērīgu ietekmi uz satiksmes plūsmu robežšķērsošanas vietās un ietekmi uz Savienības vispārējo budžetu;

i) novērtējumu par meklējumiem Interpola datubāzēs, izmantojot *ESP*, tostarp informāciju par atbilstību skaitu Interpola datubāzēs un informāciju par visām atklātajām problēmām.

Vispārējā izvērtējumā saskaņā ar šā punkta pirmo daļu iekļauj visus vajadzīgos ieteikumus. Komisija izvērtēšanas ziņojumu nosūta Eiropas Parlamentam, Padomei, Eiropas Datu aizsardzības uzraudzītājam un Eiropas Savienības Pamattiesību aģentūrai.

5. Līdz 2020. gada 12. jūnijam un katru gadu pēc tam, kamēr vēl nav pieņemti 68. pantā minētie Komisijas īstenošanas akti, Komisija iesniedz ziņojumu Eiropas Parlamentam un Padomei par stāvokli sagatavošanas darbos šīs regulas pilnai īstenošanai. Minētajā ziņojumā iekļauj arī detalizētu informāciju par radītajām izmaksām un informāciju par jebkādiem riskiem, kas var ietekmēt kopējās izmaksas.

6. Divus gadus pēc *MID* darbības sākuma saskaņā ar 68. panta 4. punktu Komisija sagatavo analīzi par *MID* ietekmi uz tiesībām uz nediskriminēšanu. Pēc šā pirmā ziņojuma analīze par *MID* ietekmi uz tiesībām uz nediskriminēšanu ir daļa no šā panta 4. punkta b) apakšpunktā minētās analīzes.

7. Dalībvalstis un Eiropols sniedz *eu-LISA* un Komisijai informāciju, kas vajadzīga, lai izstrādātu 3. līdz 6. punktā minētos ziņojumus. Šī informācija neapdraud darba metodes, un tajā neietver informāciju, kas atklāj izraudzīto iestāžu avotus, darbiniekus vai izmeklēšanas.

8. *eu-LISA* sniedz Komisijai informāciju, kas vajadzīga, lai izstrādātu 4. punktā minēto vispārējo izvērtējumu.

9. Ievērojot valsts tiesību aktus par konfidenciālas informācijas publicēšanu un neskarot ierobežojumus, kas vajadzīgi, lai aizsargātu drošību un sabiedrisko kārtību, nepieļautu noziegumus un garantētu, ka netiek apdraudēta valsts veikta izmeklēšana, katra dalībvalsts un Eiropols sagatavo gada ziņojumus par to, cik efektīva ir bijusi piekļuve *CIR* glabātajiem datiem, kas īstenota nolūkā novērst, atklāt vai izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus, un šajos ziņojumos iekļauj informāciju un statistikas datus par:

a) aplūkošanas konkrēto mērķi, ietverot teroristu nodarījuma vai cita smaga noziedzīga nodarījuma veidu;

b) pamatotajiem iemesliem, kas norādīti saistībā ar pamatotajām aizdomām, ka uz aizdomās turēto personu, nodarījuma izdarītāju vai cietušo attiecas Regula (ES) Nr. 603/2013;

c) pieprasījumu skaitu piekļuvei *CIR*, kuras nolūks ir novērst, atklāt un izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus;

d) to lietu skaitu un veidu, kurās ir bijusi sekmīga identifikācija;

e) informāciju par to, cik bieži bija vajadzīgi izņēmumi steidzamības gadījumos un cik bieži tie tika izmantoti, tostarp par gadījumiem, kad centrālā piekļuves punkta veiktajā *ex post* verifikācijā netika atzīts, ka šāds ārkārtas steidzamības gadījums pastāvēja.

Dalībvalstu un Eiropola sagatavotos gada ziņojumus nosūta Komisijai līdz nākamā gada 30. jūnijam.

10. Dalībvalstīm dara pieejamu tehnisku risinājumu, kura nolūks ir pārvaldīt 22. pantā minētos lietotāju piekļuves pieprasījumus un atvieglot informācijas vākšanu saskaņā ar šā panta 7. un 9. punktu nolūkā sagatavot minētajos punktos minētos ziņojumus un statistiku. Komisija pieņem īstenošanas aktus, nosakot tehniskā risinājuma specifikācijas. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 70. panta 2. punktā.

75. pants

Stāšanās spēkā un piemērošana

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

Šīs regulas noteikumus par *ESP* piemēro no dienas, ko Komisija noteikusi saskaņā ar 68. panta 1. punktu.

Šīs regulas noteikumus par kopējo *BMS* piemēro no dienas, ko Komisija noteikusi saskaņā ar 68. panta 2. punktu.

Šīs regulas noteikumus par *CIR* piemēro no dienas, ko Komisija noteikusi saskaņā ar 68. panta 3. punktu.

Šīs regulas noteikumus par *MID* piemēro no dienas, ko Komisija noteikusi saskaņā ar 68. panta 4. punktu.

Šīs regulas noteikumus par automatizētajiem datu kvalitātes kontroles mehānismiem un procedūrām, kopējiem datu kvalitātes indikatoriem un minimālajiem datu kvalitātes standartiem piemēro no dienas, ko Komisija noteikusi saskaņā ar 68. panta 5. punktu.

Šīs regulas noteikumus par *CRRS* piemēro no dienas, ko Komisija noteikusi saskaņā ar 68. panta 6. punktu.

Šīs regulas 6., 12., 17., 25., 38., 42., 54., 56., 58., 66., 67., 69., 70., 71. un 73. pantu un 74. panta 1. punktu piemēro no 2019. gada 11. jūnija.

Attiecībā uz *Eurodac* šo regulu piemēro no dienas, kad kļūst piemērojama Eiropas Parlamenta un Padomes Regulas (ES) Nr. 603/2013 pārstrādātā versija.

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

Briselē, 2019. gada 20. maijā

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*
A. TAJANI	G. CIAMBA

ISSN 1977-0715 (elektroniskais izdevums)
ISSN 1725-5112 (papīra izdevums)

Eiropas Savienības Publikāciju birojs
2985 Luksemburga
LUKSEMBURGA

LV