

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2019/817**(2019. gada 20. maijs),****ar ko izveido satvaru ES informācijas sistēmu sadarbībai 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 vienkāršākas robežu un drošības informācijas sistēmas" uzsvēra nepieciešamību uzlabot Savienības datu pārvaldības arhitektūru robežu pārvaldības un drošības jomā. Ar šo paziņojumu tika sākti virzība uz ES drošības, robežu un migrācijas pārvaldības informācijas sistēmu sadarbības 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 sadarbības risinājumus, tieslietu un iekšlietu jomā Padome apzināja dažādas tiesiskas, tehniskas un operatīvas problēmas ES informācijas sistēmu sadarbībā 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 sadarbības 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 sadarbību.
- (5) Augsta līmeņa ekspertu grupa informācijas sistēmu un sadarbības jautājumos 2017. gada 11. maija galīgajā ziņojumā secināja, ka ir nepieciešams un tehniski iespējams sākt darbu pie praktiskiem sadarbības risinājumiem un ka sadarbība principā var gan sniegt operatīvos ieguvumus, gan to var izstrādāt atbilstīgi datu aizsardzības prasībām.

⁽¹⁾ OVC 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⁾ OVC 101, 16.3.2018., 116. lpp.

- (6) 2017. gada 16. maija paziņojumā "Septītais progressa 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 sadarbības 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 sadarbības risinājumus, kā ierosinājusi augsta līmeņa ekspertu grupa.
- (8) Eiropadome savos 2017. gada 23. jūnija secinājumos uzsvēra nepieciešamību uzlabot sadarbību 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 sadarbības jautājumos.
- (9) Lai uzlabotu pārbaudu 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 sadarbība 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 sadarbības 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 sadarbībai 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) Sadarbības komponentiem būtu jāaptver IIS, VIS, ETIAS, Eurodac, SIS un ECRIS-TCN. Tiem būtu jāaptver arī Eiropola dati, bet vienīgi tiktāl, lai Eiropola datus varētu veikt vaicājumus vienlaikus ar minētajām ES informācijas sistēmām.
- (12) Sadarbības 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 datus 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 jāpieņem 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 datus 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 jāsauglabā 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 datus 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 sadarbības 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 jā sastāv no datiem, kas atvasināti faktisko biometrisko paraugu iezīmju izgūšanas rezultātā un iegūti tādā veidā, ka šis izgūšanas process ir neatgriezenisks. Biometriskās veidnes būtu jā iegūst no biometriskajiem datiem, taču nevajadzētu būt iespējamam tos pašus biometriskos datus iegūt no biometriskajām veidnēm. Tā kā plaukstu 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 jā glabā DNS profili vai biometriskās veidnes, kas iegūtas no plaukstu nospiedumu datiem.
- (20) Biometriskie dati ir sensitīvi personas dati. Ar šo regulu būtu jā nosaka 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 jā atvieglo 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 sadarbībai būtu jā palīdz pareizi identificēt personas, kas tajās atrodamas. CIR būtu jā glabā 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 jā glabā tikai tie personas dati, kas ir noteikti vajadzīgi, lai veiktu precīzu identitātes pārbaudi. CIR reģistrētie personas dati būtu jā glabā ne ilgāk, kā tas ir noteikti nepieciešams pamatā esošo sistēmu nolūkos, un tie būtu automātiski jā dzēš 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 jā kavē 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 jā glabā vienā vienīgā vietā visa ar personu saistītā identitātes informācija un jā dara tā pieejama pienācīgi pilnvarotiem galalietotājiem.
- (25) Tādējādi CIR būtu jā atvieglo un jā racionalizē 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 jā izveido kopīga personu, kuras reģistrētas IIS, VIS, ETIAS, Eurodac un ECRIS-TCN, identitātes datu, ceļošanas dokumentu datu un biometrisku datu krātuve. Tam vajadzētu ietilpt minēto sistēmu tehniskajā arhitektūrā un darboties kā to kopīgam komponentam identitātes datu, ceļošanas dokumentu datu un biometrisku datu, kurus tās apstrādā, glabāšanai un vaicājumu veikšanai tajās.
- (27) Visi CIR esošie ieraksti būtu loģiski jā nodala, automātiski marķējot katru ierakstu ar tās pamatā esošās sistēmas nosaukumu, kurai minētais ieraksts pieder. Kontrolei attiecībā uz piekļuvi CIR būtu jā izmanto 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 tiesās 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 pārbaudes 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 Eiropalam efektīvāk pieprasīt piekļūvi 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 verificācijas, 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 iespējamās saiknes, kuru pamatā ir biometriskie dati. CIR un SIS būtu jāizmanto ESP, lai atklātu iespējamās 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 nerādītu 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 iecelšanu, un visi lēmumi par iecelšanas 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 diskretu pārbaudi, izmeklēšanas pārbaudi vai īpašu pārbaudi 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 jāvērsas, 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 jāpiesūta tikai un vienīgi nolūkā ļaut minētajai iestādei vai aģentūrai atklāt potenciālus gadījumus, kad dati ir saistīti nepareizi vai tie apstrādāti MID, CIR un SIS, pārskatot 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 robežpārbaudi jomā un ar kuru groza Konvenciju, ar ko īsteno Šengenas nolikumu, 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 pienākamam 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 sadarbības komponentos. Šādu datu kvalitātes standartu mērķim vajadzētu būt panākt, ka ES informācijas sistēmas un sadarbības komponenti var automatiski identificēt acīmredzami kļūdainus vai nekonsistentus 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 pienākamam 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 sadarbību, 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 jaunajos 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 jānodrošina 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 jāpiespīķir tieša piekļuve ES informācijas sistēmās vai sadarbības komponentos glabātiem personas datiem.
- (53) Personas datu apstrādei sadarbības 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 sadarbības 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 pārziņim 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 sadarbības 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 sadarbības 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 sadarbības 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* sadarbības komponentu izstrādes gaitā būtu jāievēro integrētas privātuma aizsardzības un privātuma aizsardzības pēc noklusējuma principi.
- (62) Šajā regulā paredzēto sadarbības komponentu īstenošana ietekmēs to, kā robežšķērsošanas vietās tiek veiktas pārbaudes. Šī ietekme izrietēs no pastāvošo Regulas (ES) 2016/399 noteikumu un šajā regulā paredzēto sadarbības 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 iecelšanas 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 iecelšanas/izceļošanas sistēmu (IIS), lai reģistrētu to trešo valstu valstspiederīgo iecelšanas un izceļošanas datus un iecelšanas 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 sadarbības 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 sadarbības 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 sadarbības 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 šī 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 sadarbības 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 sadarbības 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 pievienošanu 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 PIENĒMUŠI 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 sadarbības nodrošināšanai starp iecelšanas/izceļošanas sistēmu (IIS), vīzu informācijas sistēmu (VIS), Eiropas ceļošanas informācijas un atļauju sistēmu (ETIAS), Eurodac, Šengenas Informācijas sistēmu (SIS) un Eiropas Sodamības 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 pievienošanu 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 pārvietošanu (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 Eiropas 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 sadarbībai 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 sadarbības komponentus:
 - a) Eiropas meklēšanas portāls (*ESP*);
 - b) kopējs biometrisku datu salīdzināšanas pakalpojums (kopējais *BMS*);
 - c) kopējs identitātes repositorijs (*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 repositorijs (*CRRS*) un ir noteikti dalībvalstu un Eiropas Aģentūras lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) pienākumi attiecībā uz sadarbības komponentu uzbūvi, izstrādi un darbību.
4. Ar šo regulu arī pielāgo procedūras un nosacījumus, ko piemēro dalībvalstu izraudzīto iestāžu un Eiropas Savienības Aģentūras tiesībsardzības 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 sadarbību, šai regulai ir šādi mērķi:
 - a) uzlabot robežpārbaudu 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 piekļuvei *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 atbilstība, 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 procedūram 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 datus 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 datus 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 datus 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 datus 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 datus 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:

- dalībvalsts iestāde vai Savienības aģentūra, kas veikusi vaicājumu, un izmantotais ESP profils;
- vaicājuma datums un laiks;
- 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 nepieklūtu 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 plaukstu nospiedumu datus;
- d) dati, kas minēti Regulas (ES) 2018/1860 4. panta 1. punkta u) un v) apakšpunktā, izņemot plaukstu 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 biometrisku 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 veikspējas prasības un praktisko kārtību, kā uzraudzīt kopējā BMS veikspēju, 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

Biometrisku datu meklēšana ar kopējā biometrisku 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 biometrisku 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 biometrisku 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 biometrisku 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 nepieklūtu 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 ietvertu 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 jaunus 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 likumdeviem 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 sāka 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 likumdeviem 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 legislatīvos pasākumus. To darot, dalībvalstis ņem vērā, ka ir jāizvairās no jebkādas trešo valstu valstspiederīgo diskriminācijas. Ar šādiem legislatīviem pasākumiem konkrētā precīzā identifikācijas mērķus atbilstīgi 2. panta 1. punkta b) un c) apakšpunktā minētajiem mērķiem. Minētās dalībvalstis izraugās kompetentās policijas iestādes un nosaka šādu pārbaūžu procedūras, nosacījumus un kritērijus.

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

21. pants

Pieklūve 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 pieklūve 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 pieklūve 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 atsaucēs 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 pieklūves pieprasījuma iesniegšanas nolūkiem, ievērojot nosacījumus un procedūras, kas ir noteiktas attiecīgajos tiesību instrumentos, kuri reglamentē šādu pieklūvi.

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

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

3. Pilnīga pieklūve 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 pieklūvi.

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 nepieklūtu 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 datus, 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:
- centrāla infrastruktūra, kas glabā saiknes un atsauces uz ES informācijas sistēmām;
 - 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:
- 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;
 - Regulas (EK) Nr. 767/2008 6. panta 1. punktā minētajām vīzu iestādēm, kad *VIS* izveido vai atjaunina pieteikuma datni saskaņā ar minēto regulu;
 - ETIAS* centrālajai vienībai un *ETIAS* valsts vienībām, kad veic Regulas (ES) 2018/1240 22. un 26. pantā minēto apstrādi;
 - 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 datus, 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 diskretu pārbaudi, izmeklēšanas pārbaudi vai īpašu pārbaudi 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 dzeltēta saikne, tad minētā iestāde veic papildu pārbaudes. Minētajai iestādei tikai 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 biometrisku 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 biometrisku 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 atšķirīgu 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 biometrisku 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. Neskatot Regulas (ES) 2018/1860, (ES) 2018/1861 un (ES) 2018/1862 minētos noteikumus par brīdinājumu apstrādi *SIS* un neskatot 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. 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 nepieklūtu 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 sadarbības 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 jebkādu nepieciešamo ieteikumu. 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 repositorijs

1. Izveido centrālu ziņošanas un statistikas repositorijs (*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 repositorijs, 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 repositorijs.

⁽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 sadarbības 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 nolasišanu, kopēšanu, grozīšanu vai datu nesēju izņemšanu;
 - d) novērstu datu nesankcionētu ievadišanu, 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 sadarbības 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 sadarbības komponentos, kad, kas un kādam mērķim tos ir apstrādājis;
 - j) nodrošinātu, jo īpaši ar pienācīgu šifrēšanas paņēmieni palīdzību, ka laikā, kad personu datus pārraida uz sadarbības 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 sadarbības 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 jaunus 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 sadarbības komponentam.

43. pants

Drošības incidenti

1. Jebkuru notikumu, kas ietekmē vai var ietekmēt sadarbības 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 sadarbības 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 sadarbības 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 sadarbības 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 sadarbības 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 pārziņi 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 sadarbības komponentos vai kurus apstrādā vai kuriem piekļūst ar sadarbības 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 sadarbības 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 sadarbības 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 sadarbības 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 sadarbības 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 sadarbības 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 sadarbības komponentu centrālās infrastruktūras ekspluatē saskaņā ar šo regulu.

2. *eu-LISA* savos tehniskajos centros mitina sadarbības 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 sadarbības komponentu izstrādi un par jebkādiem pielāgojumiem, kas vajadzīgi, lai izveidotu sadarbību 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 sadarbības 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 sadarbības izveides un ir paredzēti šajā regulā.

eu-LISA izstrādā un ievieš sadarbības 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 sadarbības jautājumos priekšsēdētājs, viens loceklis, kas pārstāv *eu-LISA* un ko iecēlis tās izpilddirektors, un viens Komisijas iecelts loceklis. *eu-LISA* valdes ieceltos locekļus ievēl 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 sadarbības komponentos.

5. Programmu vadības valde tiekas regulāri un vismaz trīs reizes ceturksnī. Tā nodrošina sadarbības 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 sadarbības 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 sadarbības jautājumos regulāri tiekas līdz sadarbības 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 sadarbības komponenta darbības uzsākšanas *eu-LISA* ir atbildīga par sadarbības 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.

Sadarbības komponentu tehniskā pārvaldība ir visi tie uzdevumi un tehniskie risinājumi, kuri vajadzīgi, lai 24 stundas diennaktī 7 dienas nedēļā nodrošinātu sadarbības 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 sadarbības 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 noteikumus, *eu-LISA* piemēro pienācīgus noteikumus par dienesta noslēpumu vai citas līdzvērtīgas konfidencialitātes prasības visiem saviem darbiniekiem, kuriem jāstrādā ar sadarbības 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 sadarbības 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 sadarbības 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 legislatīvo 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 sadarbībai 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 datus un ceļošanas dokumenta datus. 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 sadarbībai 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 sadarbībai 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 repositorijs (*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 spiedienu 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 sadarbībai 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 Piekļūvi *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 datus 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 pārbaudi vai īpašu pārbaudi 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 repositorijs” aizstāj ar vārdiem “Regulas (ES) 2019/817 39. pantā minētais centrālais ziņošanas un statistikas repositorijs, 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 robežpārbaucēju efektivitāti un palīdzēt ETIAS centrālajai vienībai un ETIAS valsts vienībām apstrādāt ceļošanas atļauju pieteikumus.”;

17) regulas 84. panta 4. punktam pievieno šādu daļu:

“Katrās 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 sadarbībai 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 sadarbībai 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 sadarbības 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 sadarbības 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 sadarbības 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 sadarbības 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 sadarbīgai 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 automatiskajiem 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, Eiropalam 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 sadarbībai 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 sadarbībai 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 robežpārbaucēju 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 robežpārbaucēju organizāciju un ilgumu.

68. pants

Pārejas periods, ko piemēro noteikumiem par piekļuvi kopējam identitātes repositorijs 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 sadarbības 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 sadarbības 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 Sadarbības padomdevēju grupu. Sadarbības 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 sadarbības komponentu tehnisko izmantošanu.

Dalībvalstu iestādes un Savienības aģentūras nodrošina saviem darbiniekiem, kas ir pilnvaroti apstrādāt datus, izmantojot sadarbības komponentus, atbilstīgas apmācības programmas par datu drošību, datu kvalitāti, datu aizsardzības noteikumiem, datu apstrādei piemērojāmām 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 sadarbības 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 sadarbības 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 sadarbības komponentu izstrādi un to savienošanu ar valsts vienoto saskarni, ņemot vērā ar plānošanu un izmaksām saistītos mērķus, un lai uzraudzītu sadarbības 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 sadarbības 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 sadarbības komponenta darbības uzsākšanas saskaņā ar 72. pantu un turpmāk ik pēc četriem gadiem *eu-LISA* iesniedz Eiropas Parlamentam, Padomei un Komisijai ziņojumu par sadarbības komponentu tehnisko darbību, tostarp to drošību.

4. Turklāt vienu gadu pēc katra *eu-LISA* izstrādātā ziņojuma Komisija sagatavo sadarbības 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 sadarbības 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 sadarbības komponentu pamatojuma turpmāku derīgumu;
- e) novērtējumu par sadarbības 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 jebkādam 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 jebkādas 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 konfidencialas 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:
- aplūkošanas konkrēto mērķi, ietverot teroristu nodarījuma vai cita smaga noziedzīga nodarījuma veidu;
 - 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;
 - pieprasījumu skaitu piekļuvei *CIR*, kuras nolūks ir novērst, atklāt un izmeklēt teroristu nodarījumus vai citus smagus noziedzīgus nodarījumus;
 - to lietu skaitu un veidu, kurās ir bijusi sekmīga identifikācija;
 - 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* verificācijā 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 –
priekšsēdētājs
A. TAJANI

Padomes vārdā –
priekšsēdētājs
G. CIAMBA
