

**UREDBA (EU) 2019/818 EVROPSKEGA PARLAMENTA IN SVETA****z dne 20. maja 2019****o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju policijskega in pravosodnega sodelovanja, azila ter migracij in spremembi uredb (EU) 2018/1726, (EU) 2018/1862 ter (EU) 2019/816**

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 16(2), člena 74, člena 78(2)(e), člena 79(2)(c), člena 82(1)(d), člena 85(1), člena 87(2)(a) ter člena 88(2) Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora <sup>(1)</sup>,

po posvetovanju z Odborom regij,

v skladu z rednim zakonodajnim postopkom <sup>(2)</sup>,

ob upoštevanju naslednjega:

- (1) Komisija je v svojem sporočilu z dne 6. aprila 2016 z naslovom Trdnější in pametnější informacijski sistemi za meje in varnost poudarila potrebo po izboljšanju arhitekture Unije za upravljanje podatkov za upravljanje meja in varnosti. S sporočilom se je začel proces za doseg interoperabilnosti informacijskih sistemov EU za upravljanje varnosti, meja in migracij, da bi se odpravile strukturne pomanjkljivosti teh sistemov, ki ovirajo delo nacionalnih organov, ter da bi se mejnim policistom, carinskim organom, policistom in sodnim organom zagotovile potrebne informacije.
- (2) Svet je v svojem načrtu z dne 6. junija 2016 za boljšo izmenjavo in upravljanje informacij, vključno z interoperabilnostnimi rešitvami, na področju pravosodja in notranjih zadev opredelil različne pravne, tehnične in operative izzive za interoperabilnost informacijskih sistemov EU ter pozval k iskanju rešitev.
- (3) Evropski parlament je v svoji resoluciji z dne 6. julija 2016 o strateških prednostnih nalogah v delovnem programu Komisije za leto 2017 <sup>(3)</sup> pozval k predlogom za izboljšanje in razvoj obstoječih informacijskih sistemov EU, zapolnitev informacijskih vrzeli in premik k interoperabilnosti ter predlogom za obvezno izmenjavo informacij na ravni EU, ki naj jih spremljajo nujni zaščitni ukrepi za varstvo podatkov.
- (4) Evropski svet je v svojih sklepih z dne 15. decembra 2016 pozval k nadaljnjemu napredku glede interoperabilnosti informacijskih sistemov in podatkovnih zbirk EU.
- (5) Strokovna skupina na visoki ravni za informacijske sisteme in interoperabilnost je v svojem končnem poročilu z dne 11. maja 2017 ugotovila, da so praktične rešitve za doseg interoperabilnosti potrebne in tehnično izvedljive ter da lahko interoperabilnost načeloma zagotovi operative koristi in se vzpostavi skladno z zahtevami varstva podatkov.
- (6) Komisija je v svojem sporočilu z dne 16. maja 2017 z naslovom Sedmo poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije v skladu s svojim sporočilom z dne 6. aprila 2016 ter ugotovitvami in priporočili strokovne skupine na visoki ravni za informacijske sisteme in interoperabilnost določila nov pristop k upravljanju podatkov za upravljanje meja, varnosti in migracij, v okviru katerega naj bi bili vsi informacijski sistemi EU za upravljanje varnosti, meja in migracij interoperabilni na način, ki popolnoma spoštuje temeljne pravice.

<sup>(1)</sup> UL C 283, 10.8.2018, str. 48.

<sup>(2)</sup> Stališče Evropskega parlamenta z dne 16. aprila 2019 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 14. maja 2019.

<sup>(3)</sup> UL C 101, 16.3.2018, str. 116.

- (7) Svet je v svojih sklepih z dne 9. junija 2017 o nadaljnjih ukrepih za boljšo izmenjavo informacij in zagotavljanje interoperabilnosti informacijskih sistemov EU pozval Komisijo, da izvede rešitve za interoperabilnost, ki jih je predlagala strokovna skupina na visoki ravni.
- (8) Evropski svet je v svojih sklepih z dne 23. junija 2017 poudaril potrebo po izboljšanju interoperabilnosti med podatkovnimi zbirkami in pozval Komisijo, da čim prej pripravi osnutek zakonodaje na podlagi predlogov strokovne skupine na visoki ravni za informacijske sisteme in interoperabilnost.
- (9) Da bi se izboljšali učinkovitost in uspešnost pregledov na zunanjih mejah, okrepilo preprečevanje nezakonitega priseljevanja in boj proti njemu ter prispevalo k visoki ravni varnosti na območju svobode, varnosti in pravice Unije, vključno vzdrževanju javne varnosti in javnega reda ter zagotavljanjem varnosti na ozemljih držav članic, izboljšalo izvajanje skupne vizumske politike, pomagalo pri obravnavi prošelj za mednarodno zaščito, prispevalo k preprečevanju, odkrivanju in preiskovanju terorističnih kaznivih dejanj in drugih hudih kaznivih dejanj, olajšala identifikacija neznanih oseb, ki se ne morejo same identificirati, ali neidentificiranih človeških ostankov v primeru naravne nesreče, nezgode ali terorističnega napada, s čimer bi se ohranjalo zaupanje javnosti v migracijski in azilni sistem Unije, varnostne ukrepe Unije in zmogljivosti Unije za upravljanje zunanje meje, bi bilo treba vzpostaviti interoperabilnost med informacijskimi sistemi Unije, in sicer sistemom vstopa/izstopa (SVI), vizumskim informacijskim sistemom (VIS), evropskim sistemom za potovalne informacije in odobritve (ETIAS), sistemom Eurodac, schengenskim informacijskim sistemom (SIS) in evropskim informacijskim sistemom kazenskih evidenc za državljane tretjih držav (v nadaljnjem besedilu: sistem ECRIS-TCN), da bi se ti informacijski sistemi EU in njihovi podatki med seboj dopolnjevali ob hkratnem spoštovanju temeljnih pravic posameznikov, zlasti pravice do varstva osebnih podatkov. Za doseg tega bi bilo treba kot sestavne dele interoperabilnosti vzpostaviti evropski iskalni portal (ESP), skupno storitev za ugotavljanje ujemanja biometričnih podatkov (skupna BMS), skupno odložišče podatkov o identiteti (CIR) in detektor več identitet (MID).
- (10) Interoperabilnost informacijskih sistemov EU bi morala omogočiti, da se ti sistemi med seboj dopolnjujejo, kar bi olajšalo pravilno identifikacijo oseb, vključno z neznanimi osebami, ki se ne morejo same identificirati, ali neidentificirani človeški ostanki, prispevalo k boju proti identitetnim prevaram, izboljšalo in harmoniziralo zahteve glede kakovosti podatkov zadevnih informacijskih sistemov EU, državam članicam olajšalo tehnično in operativno izvajanje informacijskih sistemov EU, okrepilo zaščitne ukrepe za varnost in varstvo podatkov, ki urejajo zadevne informacijske sisteme EU, racionaliziralo dostop do SVI, VIS, ETIAS in sistema Eurodac za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj ter podprlo namene SVI, VIS, ETIAS, sistema Eurodac, SIS in sistema ECRIS-TCN.
- (11) Sestavni deli interoperabilnosti bi morali zajemati SVI, VIS, ETIAS, sistem Eurodac, SIS in sistem ECRIS-TCN. Poleg tega bi morali zajemati tudi podatke Europol, vendar le do te mere, da se lahko po podatkih Europol poizveduje sočasno v teh informacijskih sistemih EU.
- (12) Sestavni deli interoperabilnosti bi morali obdelovati osebne podatke oseb, katerih osebni podatki se obdelujejo v osnovnih informacijskih sistemih EU in s strani Europol.
- (13) ESP bi bilo treba vzpostaviti, da bi tehnično omogočil hiter, nemoten, učinkovit, sistematičen in nadzorovan dostop organov držav članic ter agencij Unije do informacijskih sistemov EU, do podatkov Europol in do podatkovnih zbirk Mednarodne organizacije kriminalistične policije (Interpol), kolikor je to potrebno za opravljanje njihovih nalog v skladu z njihovimi pravicami dostopa. ESP bi bilo treba vzpostaviti tudi, da bi se podprli cilji SVI, VIS, ETIAS, sistema Eurodac, SIS, sistema ECRIS-TCN in podatkov Europol. Z omogočanjem vzporednega poizvedovanja v vseh zadevnih informacijskih sistemih EU, po podatkih Europol in v Interpolovih podatkovnih zbirkah, bi moral ESP delovati kot enotno okno oziroma „posrednik sporočil“ za nemoteno iskanje v različnih centralnih sistemih in pridobivanje potrebnih informacij ob popolnem spoštovanju zahtev glede nadzora dostopa in varstva podatkov osnovnih sistemov.
- (14) Zasnova ESP bi morala zagotoviti, da se pri poizvedovanju v Interpolovih podatkovnih zbirkah podatki, ki jih je uporabnik ESP uporabil za sprožitev poizvedbe, ne delijo z lastniki podatkov Interpol. Zasnova ESP bi morala zagotoviti tudi, da se v Interpolovih podatkovnih zbirkah poizveduje samo v skladu z veljavnim pravom Unije in nacionalnim pravom.

- (15) Tistim uporabnikom ESP, ki imajo pravico do dostopa do podatkov Europol v skladu z Uredbo (EU) 2016/794 Evropskega parlamenta in Sveta <sup>(4)</sup>, bi morale biti omogočeno sočasno poizvedovanje po podatkih Europol in po informacijskih sistemih EU, do katerih imajo dostop. Vsaka nadaljnja obdelava podatkov na podlagi take poizvedbe bi morala potekati v skladu z Uredbo (EU) 2016/794, vključno z omejitvami dostopa ali uporabe, ki jih naloži ponudnik podatkov.
- (16) ESP bi bilo treba razviti in konfigurirati tako, da izvedbo take poizvedbe dovoljuje le z uporabo podatkov, ki se ne nanašajo na osebe ali potne listine in so prisotni v informacijskem sistemu EU, podatkih Europol ali Interpolovih podatkovnih zbirkah.
- (17) Za zagotovitev sistematične uporabe zadevnih informacijskih sistemov EU bi se moral ESP uporabljati za poizvedovanje v CIR, SVI, VIS, ETIAS, sistemu Eurodac in sistemu ECRIS-TCN. Vendar bi bilo treba ohraniti nacionalno povezavo do različnih informacijskih sistemov EU, da se zagotovi tehnična nadomestna možnost. ESP bi morale uporabljati tudi agencije Unije za poizvedovanje v centralnem SIS v skladu s svojimi pravicami dostopa, da bi lahko opravljale svoje naloge. ESP bi moral biti dodaten način poizvedovanja v centralnem SIS, po podatkih Europol in v Interpolovih podatkovnih zbirkah, ki dopolnjuje obstoječe namenske vmesnike.
- (18) Biometrični podatki, kot so prstni odtisi in podobe obraza, so edinstveni in zato veliko bolj zanesljivi za namene ugotavljanja identitete osebe kot alfanumerični podatki. Skupna BMS bi morala biti tehnično orodje, ki naj bi okrepilo in olajšalo delo zadevnih informacijskih sistemov EU in drugih sestavnih delov interoperabilnosti. Glavni namen skupne BMS bi moral biti, da olajša identifikacijo posameznika, ki je registriran v več podatkovnih zbirkah, z uporabo enotnega tehnološkega sestavnega dela za ujemanje biometričnih podatkov posameznika po različnih sistemih namesto uporabe več sestavnih delov. Skupna BMS bi morala prispevati k varnosti ter koristim v smislu financiranja, vzdrževanja in delovanja. Vsi sistemi za samodejno identifikacijo prstnih odtisov, vključno s tistimi, ki se trenutno uporabljajo za sistem Eurodac, VIS in SIS, uporabljajo biometrične predloge, ki jih sestavljajo podatki, pridobljeni z ekstrakcijo značilnosti iz dejanskih biometričnih vzorcev. Skupna BMS bi morala združiti in hraniti vse te biometrične predloge – smiselno ločene glede na to, iz katerega informacijskega sistema podatkov izvirajo – na enem samem mestu, kar bi olajšalo primerjavo med različnimi sistemi na podlagi biometričnih predlog ter omogočilo ekonomijo obsega pri razvoju in ohranjanju centralnih sistemov EU.
- (19) Biometrične predloge, shranjene v skupni BMS, bi morali sestavljati podatki, pridobljeni z ekstrakcijo značilnosti iz dejanskih biometričnih vzorcev, in bi morale biti pridobljene na tak način, da postopka ekstrakcije ni mogoče izvesti v obratni smeri. Biometrične predloge bi morale biti pridobljene iz biometričnih podatkov, ne bi pa smelo biti mogoče iz teh biometričnih predlog pridobiti iste biometrične podatke. Ker so podatki o odtisih dlani in profili DNK shranjeni le v SIS in jih ni mogoče uporabiti za navzkrižna preverjanja s podatki v drugih informacijskih sistemih, se v skladu z načeloma nujnosti in sorazmernosti v skupni BMS ne bi smeli hraniti profili DNK ali biometrične predloge, pridobljeni iz podatkov o odtisih dlani.
- (20) Biometrični podatki so občutljivi osebni podatki. Ta uredba bi morala določati podlago in zaščitne ukrepe za obdelavo takih podatkov za namene edinstvene identifikacije zadevnih oseb.
- (21) SVI, VIS, ETIAS, sistem Eurodac in sistem ECRIS-TCN so odvisni od natančne identifikacije oseb, katerih osebni podatki se hranijo v teh sistemih. Zato bi moral CIR olajšati pravilno identifikacijo oseb, registriranih v teh sistemih.
- (22) Osebni podatki, ki se hranijo v teh informacijskih sistemih EU, se lahko nanašajo na iste osebe, vendar z različnimi ali nepopolnimi identitetami. Države članice imajo na voljo učinkovita sredstva za identifikacijo svojih državljanov ali registriranih stalnih prebivalcev na svojem ozemlju. Interoperabilnost informacijskih sistemov EU bi morala prispevati k pravilni identifikaciji oseb, prisotnih v teh sistemih. CIR bi moral hraniti osebne podatke, ki so potrebni za natančnejšo identifikacijo posameznikov, katerih podatki se hranijo v teh sistemih, vključno z njihovimi podatki o identiteti, podatki o potni listini in biometričnimi podatki ne glede na sistem, v katerem so bili ti podatki prvotno zbrani. V CIR bi bilo treba hraniti bi le osebne podatke, ki so nujno potrebni za natančno ugotavljanje identitete. Osebni podatki, evidentirani v CIR, bi se morali hraniti le, dokler je to nujno potrebno za namene osnovnih sistemov, in bi se morali samodejno izbrisati, ko se podatki izbrišejo v osnovnih sistemih v skladu z njihovim logičnim ločevanjem.

<sup>(4)</sup> Uredba (EU) 2016/794 Evropskega parlamenta in Sveta z dne 11. maja 2016 o Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) ter nadomestitvi in razveljavitvi sklepov Sveta 2009/371/PNZ, 2009/934/PNZ, 2009/935/PNZ, 2009/936/PNZ in 2009/968/PNZ (UL L 135, 24.5.2016, str. 53).

- (23) Nov postopek obdelave, ki zajema hrambo takih podatkov v CIR namesto hrambe v vsakem od ločenih sistemov, je potreben, da se omogoči povečanje natančnosti identifikacije prek samodejne primerjave in ugotavljanja ujemanja podatkov. Dejstvo, da se podatki o identiteti, podatki o potni listini in biometrični podatki hranijo v CIR, nikakor ne bi smelo ovirati obdelave podatkov za namene SVI, VIS, ETIAS, sistemu Eurodac ali sistemu ECRIS-TCN, saj bi moral biti CIR nov skupni sestavni del teh osnovnih sistemov.
- (24) Zato je treba v CIR za vsako osebo, ki je evidentirana v SVI, VIS, ETIAS, sistemu Eurodac ali sistemu ECRIS-TCN, oblikovati individualno dokumentacijo, da se doseže pravilna identifikacija osebe na schengenskem območju ter da se podpre MID za lažje ugotavljanje identitete dobrovernih potnikov in boj proti identitetnim prevaram. Individualna dokumentacija bi morala hraniti vse informacije o identiteti, povezane z osebo, na enem samem mestu in omogočiti dostop ustrezno pooblaščenim končnim uporabnikom.
- (25) Zato bi moral CIR olajšati in racionalizirati dostop organov, pristojnih za preprečevanje, odkrivanje ali preiskovanje terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, do informacijskih sistemov EU, ki niso vzpostavljeni izključno za namene preprečevanja, odkrivanja ali preiskovanja hudih kaznivih dejanj.
- (26) CIR bi moral zagotavljati skupno mesto za podatke o identiteti, podatke o potni listini in biometrične podatke oseb, registriranih v SVI, VIS, ETIAS, sistemu Eurodac in sistemu ECRIS-TCN. Vključen bi moral biti v tehnično zgradbo teh sistemov ter delovati kot skupni sestavni del teh sistemov za hrambo in poizvedovanje po podatkih o identiteti, podatkih o potni listini in biometričnih podatkih, ki jih obdelujejo.
- (27) Vse evidence v CIR bi morale biti logično ločene s samodejnim označevanjem vsake evidence z imenom osnovnega sistema, kateremu pripada. Pri nadzoru dostopa v okviru CIR bi bilo treba na podlagi teh oznak določiti, ali se dovoli dostop do evidence.
- (28) Kadar policijski organ države članice ne more identificirati osebe, ker nima potne listine ali drugega verodostojnega dokumenta, ki določa identiteto te osebe, ali kadar obstaja dvom glede podatkov o identiteti, ki jih je navedla ta oseba, ali glede verodostojnosti potne listine ali identitete njegovega imetnika, ali kadar oseba ne more ali ne želi sodelovati, bi moral imeti ta policijski organ možnost, da poizveduje v CIR z namenom identifikacije osebe. Za te namene bi morali policijski organi pridobiti prstne odtise z uporabo tehnik odvzema prstnih odtisov na kraju samem, če se postopek prične v prisotnosti te osebe. Take poizvedbe v CIR ne bi smele biti dovoljene za namene identifikacije mladoletnikov, mlajših od 12 let, razen če je to v največjo korist otroka.
- (29) Kadar biometričnih podatkov osebe ni mogoče uporabiti ali če je poizvedba na podlagi teh podatkov neuspešna, bi jo bilo treba opraviti na podlagi podatkov o identiteti osebe in podatkov o potni listini. Kadar poizvedba pokaže, da se podatki tej osebi hranijo v CIR, bi morali imeti organi držav članic dostop do CIR, da vpogledajo v podatke o identiteti in podatke o potni listini te osebe ne da bi CIR navedel, kateremu informacijskemu sistemu EU podatki pripadajo.
- (30) Države članice bi morale sprejeti nacionalne zakonodajne ukrepe za imenovanje organov, ki so pristojni za ugotavljanje identitete z uporabo CIR, ter za določitev postopkov, pogojev in meril za tako ugotavljanje, ki bi morali slediti načelu sorazmernosti. Zlasti bi bilo treba v nacionalnem pravu določiti pooblastilo, da člani navedenih organov med ugotavljanjem identitete navzoče osebe zberejo njene biometrične podatke.
- (31) Ta uredba bi morala uvesti tudi novo možnost za racionaliziran dostop organov, ki jih imenujejo države članice, pristojnih za preprečevanje, odkrivanje ali preiskovanje terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, in Europol do podatkov v SVI, VIS, ETIAS ali sistemu Eurodac, ki niso le podatki o identiteti ali podatki o potni listini. Taki podatki so lahko v posameznem primeru potrebni za preprečevanje, odkrivanje ali preiskovanje terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, kadar obstaja utemeljen razlog za domnevo, da bo vpogled vanje prispeval k preprečevanju, odkrivanju ali preiskovanju terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, zlasti kadar obstaja sum, da je osumljenec, storilec ali žrtev terorističnega kaznivega dejanja ali drugega hudega kaznivega dejanja oseba, katere podatki se hranijo v SVI, VIS, ETIAS ali sistemu Eurodac.

- (32) Popoln dostop do podatkov v informacijskih sistemih EU, ki je potreben za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, ki presega dostop le do podatkov o identiteti ali podatkov o potni listini, ki so v CIR, bi morali še naprej urejati pravni instrumenti, ki se uporabljajo. Imenovani organi, pristojni za preprečevanje, odkrivanje ali preiskovanje terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, in Europol ne vedo vnaprej, kateri informacijski sistemi EU vsebujejo podatke o osebah, v zvezi s katerimi morajo opraviti iskanje. To povzroča zamude in neučinkovitost. Zato bi moralo biti končnemu uporabniku, ki ga pooblasti imenovani organ, dovoljeno videti, v katerem od teh informacijskih sistemov EU so evidentirani podatki, ki so rezultat poizvedbe. Tako bi bil zadevni sistem po samodejnem preverjanju obstoja ujemanja v njem (tako imenovana funkcija označitve ujemanja) označen.
- (33) V tej zvezi se odgovor ne bi smel razlagati ali uporabiti kot podlaga ali razlog za sklepanje zaključkov o osebi ali za sprejemanje ukrepov v zvezi z osebo, temveč se lahko uporabi le za namen vložitve zahtevka za dostop do osnovnih informacijskih sistemov EU v skladu s pogoji in postopki iz zadevnih pravnih instrumentov, ki urejajo tak dostop. Za vsak tak zahteve bi moralo veljati poglavje VII te uredbe in, kot je ustrezno, Uredba (EU) 2016/679 Evropskega parlamenta in Sveta <sup>(5)</sup>, Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta <sup>(6)</sup> ali Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta <sup>(7)</sup>.
- (34) V splošnem bi morali imenovani organi ali Europol zahtevati popoln dostop do vsaj enega od zadevnih informacijskih sistemov EU, kadar označitev ujemanja pokaže, da so podatki zabeleženi v sistemu Eurodac. Kadar se ta popolni dostop izjemoma ne zahteva, na primer zato, ker so imenovani organi ali Europol podatke že pridobili na drug način ali pa pridobivanje podatkov ni več dovoljeno na podlagi nacionalnega prava, bi bilo treba evidentirati utemeljitev, zakaj dostop ni zahtevan.
- (35) V dnevnikih poizvedb v CIR bi moral biti naveden namen poizvedb. Kadar se taka poizvedba opravi na podlagi vpogledu v podatke v dveh korakih, bi morali dnevniki vsebovati sklic na nacionalno dokumentacijo o preiskavi ali primeru, s čimer se navede, da je bila taka poizvedba sprožena za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj.
- (36) Pri poizvedbi v CIR, ki jo imenovani organi in Europol opravijo, da bi prejeli odgovor z označitvijo ujemanja, ki navaja, da so podatki evidentirani v SVI, VIS, ETIAS ali sistemu Eurodac, je potrebna samodejna obdelava osebnih podatkov. Označitev ujemanje ne bi smela razkriti osebnih podatkov zadevnega posameznika, razen navedbe, da se nekateri njegovi podatki hranijo v enem od sistemov. Pooblaščen končni uporabnik ne bi smel sprejeti nobene negativne odločitve glede zadevnega posameznika zgolj na podlagi označitve ujemanja. Zato bo dostop končnega uporabnika do označitve ujemanja pomenil zelo omejen poseg v pravico do varstva osebnih podatkov zadevnega posameznika, ob enem pa imenovanim organom in Europol omogočil, da učinkoviteje zahtevajo dostop do osebnih podatkov.
- (37) MID bi bilo treba vzpostaviti, da bi se podprli delovanje CIR ter cilji SVI, VIS, ETIAS, sistema Eurodac, SIS in sistema ECRIS-TCN. Za učinkovito doseganje ciljev vseh teh informacijskih sistemov EU je potrebna natančna identifikacija posameznikov, katerih osebni podatki se hranijo v njih.
- (38) Za boljše doseganje ciljev informacijskih sistemov EU bi morali imeti organi, ki te sisteme uporabljajo, možnost dovolj zanesljivo preveriti identitete oseb, katerih podatki se hranijo v različnih sistemih. Niz podatkov o identiteti ali podatkov o potni listini je lahko v posameznem sistemu napačen, nepopoln ali lažen in trenutno

<sup>(5)</sup> Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

<sup>(6)</sup> Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

<sup>(7)</sup> Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

ni nobenega načina za odkrivanje napačnih, nepopolnih ali lažnih podatkov o identiteti ali podatkov o potni listini s primerjavo s podatki, ki se hranijo v drugem sistemu. Za izboljšanje tega stanja je potreben tehnični instrument na ravni Unije, ki omogoča natančno identifikacijo oseb za te namene.

- (39) MID bi moral ustvariti in hraniti povezave med podatki v različnih informacijskih sistemih EU za odkrivanje več identitet za lažje ugotavljanje identitete dobrovernih potnikov in boj proti identitetnim prevaram. Vsebovati bi moral le povezave med podatki o posameznikih, ki so prisotni v več kot enem informacijskem sistemu EU. Povezani podatki bi morali biti strogo omejeni na podatke, potrebne za preverjanje, ali je oseba v različnih sistemih upravičeno ali neupravičeno evidentirana z različnimi identitetami, ali za pojasnitev, da osebi s podobnimi podatki o identiteti nista nujno ista oseba. Obdelava podatkov prek ESP in skupne BMS za povezovanje individualne dokumentacije med različnimi sistemi bi morala biti minimalna in tako omejena na odkrivanje več identitet, ki se opravi, ko se enemu od sistemov, ki hranijo podatke v CIR, ali SIS dodajo novi podatki. MID bi moral vključevati zaščitne ukrepe proti morebitni diskriminaciji in neugodnim odločitvam glede oseb z več zakonitimi identitetami.
- (40) Ta uredba določa nove postopke obdelave podatkov za pravilno identifikacijo zadevnih oseb. To pomeni poseg v njihove temeljne pravice, kot so zaščitene s členoma 7 in 8 Listine Evropske Unije o temeljnih pravicah. Ker je učinkovito izvajanje informacijskih sistemov EU odvisno od pravilne identifikacije zadevnih posameznikov, je tak poseg utemeljen z enakimi cilji, zaradi katerih je bil vzpostavljen vsak od teh sistemov, učinkovitim upravljanjem meja Unije, notranjo varnostjo Unije ter učinkovitim izvajanjem azilne in vizumske politike Unije.
- (41) ESP in skupna BMS bi morala primerjati podatke o osebah v CIR in SIS, kadar nacionalni organ ali agencija Unije ustvari ali naloži novo evidenco. Taka primerjava bi morala biti samodejna. CIR in SIS bi morala morebitne povezave na podlagi biometričnih podatkov zaznati prek skupne BMS. CIR in SIS bi morala morebitne povezave na podlagi alfanumeričnih podatkov zaznati prek ESP. CIR in SIS bi morala biti zmožna odkriti enake ali podobne podatke o osebi, ki se hranijo v različnih sistemih. V takem primeru bi bilo treba vzpostaviti povezavo, ki označuje, da gre za isto osebo. CIR in SIS bi morala biti konfigurirana tako, da se majhne napake pri prečkovanju ali črkovanju odkrijejo na način, ki ne ustvarja neupravičenih ovir za zadevno osebo.
- (42) Nacionalni organ ali agencija Unije, ki je evidencialni podatke v zadevnem informacijskem sistemu EU, bi moral potrditi ali spremeniti povezave. Ta nacionalni organ ali agencija Unije bi morala imeti dostop do podatkov, ki se hranijo v CIR ali SIS in v MID, za namene ročnega preverjanja različnih identitet.
- (43) Ročno preverjanje različnih identitet bi moral zagotoviti organ, ki je evidencialni ali posodobil podatke, ki so privedli do ujemanja, zaradi katerega je bila vzpostavljena povezava s podatki, ki se hranijo v drugem informacijskem sistemu EU. Organ, ki je pristojen za ročno preverjanje različnih identitet, bi moral oceniti, ali obstaja več identitet, ki se upravičeno ali neupravičeno nanašajo na isto osebo. Tako oceno bi bilo treba po možnosti opraviti v prisotnosti zadevnih oseb in po potrebi z zahtevo po dodatnih pojasnilih ali informacijah. Oceno bi bilo treba opraviti ter brez odlašanja in v skladu s pravnimi zahtevami glede točnosti informacij po pravu Unije in nacionalnem pravu.
- (44) Za povezave, pridobljene prek SIS v zvezi z razpisi ukrepov za osebe, za katere se zahteva prijetje zaradi predaje ali izročitve, za pogršane ali ranljive osebe, za osebe, iskane zaradi sodelovanja v sodnem postopku ali za osebe zaradi prikrite kontrole, poizvedovalne kontrole ali namenske kontrole, bi moral biti organ, ki je pristojen za ročno preverjanje različnih identitet, urad SIRENE države članice, ki je izdala razpis ukrepa. Te kategorije razpisov ukrepov v SIS so občutljive in se ne bi smele nujno deliti z organi, ki so evidencialni ali posodobili podatke, ki so

povezani z njimi v enem od drugih informacijskih sistemov EU. Vzpostavitev povezave s podatki v SIS ne bi smela posegati v ukrepe, ki jih je treba sprejeti v skladu z uredbami (EU) 2018/1860 <sup>(8)</sup>, (EU) 2018/1861 <sup>(9)</sup> in (EU) 2018/1862 <sup>(10)</sup> Evropskega parlamenta in Sveta.

- (45) Vzpostavitev takih povezav zahteva preglednost v odnosu do posameznikov, na katere to vpliva. Za lažje izvajanje potrebnih zaščitnih ukrepov v skladu z veljavnimi pravili Unije o varstvu podatkov bi bilo treba posameznike, za katere velja rdeča povezava ali bela povezava po ročnem preverjanju različnih identitet, pisno obvestiti brez poseganja v omejitve za zaščito varnosti in javnega reda, preprečevanje kaznivih dejanj ter zagotovitev, da niso ogrožene nacionalne preiskave. Ti posamezniki bi morali prejeti enotno identifikacijsko številko, s katero bi lahko ugotovili, na kateri organ bi se morali obrniti za uveljavljanje svojih pravic.
- (46) Kadar je vzpostavljena rumena povezava, bi moral imeti organ, odgovoren za ročno preverjanje različnih identitet, dostop do MID. Kadar obstaja rdeča povezava, bi morali organi držav članic in agencije Unije, ki imajo dostop do vsaj enega informacijskega sistema EU, vključenega v CIR, ali do SIS, imeti dostop do MID. Rdeča povezava bi morala navajati, da oseba uporablja različne identitete na neupravičen način ali da oseba uporablja identiteto nekoga drugega.
- (47) Kadar med podatki v dveh informacijskih sistemih obstaja bela ali zelena povezava, bi morali organi držav članic in agencije Unije imeti dostop do MID, kadar ima zadevni organ ali agencija dostop do obeh informacijskih sistemov. Tak dostop bi bilo treba odobriti le zato, da lahko ta organ ali agencija odkrije morebitne primere, v katerih so bili podatki povezani nepravilno ali obdelani v MID, CIR in SIS v nasprotju s to uredbo, ter da se sprejmejo potrebni ukrepi za izboljšanje stanja ter povezava posodobi ali izbriše.
- (48) Agencija Evropske unije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (eu-LISA) bi morala vzpostaviti samodejne mehanizme za nadzor kakovosti podatkov in skupne kazalnike kakovosti podatkov. Poleg tega bi morala biti eu-LISA odgovorna za razvoj centralne zmogljivosti za spremljanje kakovosti podatkov ter pripravo rednih poročil o analizi podatkov za izboljšanje nadzora nad izvajanjem informacijskih sistemov EU s strani držav članic. Skupni kazalniki kakovosti podatkov bi morali vključevati minimalne standarde kakovosti za hrambo podatkov v informacijskih sistemih EU ali sestavnih delih interoperabilnosti. Cilj takih standardov kakovosti podatkov bi moral biti, da informacijski sistemi EU in sestavni deli interoperabilnosti samodejno odkrijejo očitno nepravilne ali nedosledne predložene podatke, da bi lahko država članica izvora podatkov slednje preverila in izvedla vse potrebne popravne ukrepe.
- (49) Komisija bi morala oceniti poročila eu-LISA o kakovosti in po potrebi izdati priporočila državam članicam. Države članice bi morale biti odgovorne za pripravo akcijskega načrta, v katerem bi bili opisani ukrepi za odpravo morebitnih pomanjkljivosti v kakovosti podatkov, in bi morale redno poročati o njegovem napredku.
- (50) Univerzalni format sporočil (UMF) bi moral služiti kot standard za strukturirano čezmejno izmenjavo informacij med informacijskimi sistemi, organi ali organizacijami na področju pravosodja in notranjih zadev. V UMF bi bilo treba opredeliti skupno besedišče in logične strukture za pogosto izmenjane informacije, da bi se omogočilo dosledno in semantično enakovredno ustvarjanje in branje vsebine izmenjav, s čimer bi se olajšala interoperabilnost.
- (51) Izvajanje standarda UMF bi se lahko preučilo za VIS, SIS in katere koli druge obstoječe ali nove modele za čezmejno izmenjavo informacij ter informacijske sisteme na področju pravosodja in notranjih zadev, ki jih razvijejo države članice.

<sup>(8)</sup> Uredba (EU) 2018/1860 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o uporabi schengenskega informacijskega sistema za vračanje nezakonito prebivajočih državljanov tretjih držav (UL L 312, 7.12.2018, str. 1).

<sup>(9)</sup> Uredba (EU) 2018/1861 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju mejnih kontrol, o spremembi Konvencije o izvajanju Schengenskega sporazuma ter o spremembi in razveljavitvi Uredbe (ES) št. 1987/2006 (UL L 312, 7.12.2018, str. 14).

<sup>(10)</sup> Uredba (EU) 2018/1862 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi in razveljavitvi Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (ES) št. 1986/2006 Evropskega parlamenta in Sveta in Sklepa Komisije 2010/261/EU (UL L 312, 7.12.2018, str. 56).

- (52) Centralni register za poročanje in statistične podatke (CRRS) bi bilo treba vzpostaviti zaradi ustvarjanja medsystemske statistične podatke in analitičnega poročanja za politične in operativne namene ter namene kakovosti podatkov, v skladu z veljavnimi pravnimi instrumenti. CRRS bi morala vzpostaviti, izvajati in gostiti eu-LISA na svojih tehničnih lokacijah. Vsebovati bi moral anonimizirane statistične podatke iz informacijskih sistemov EU, CIR, MID in skupne BMS. Podatki v CRRS ne bi smeli omogočati identifikacije posameznikov. eu-LISA bi morala podatke samodejno anonimizirati in take anonimizirane podatke evidentirati v CRRS. Postopek anonimizacije podatkov bi moral biti samodejen, osebje eu-LISA pa ne bi smelo imeti neposrednega dostopa do osebnih podatkov, ki se hranijo v informacijskih sistemih EU ali sestavnih delih interoperabilnosti.
- (53) Za obdelavo osebnih podatkov za namen interoperabilnosti na podlagi te uredbe s strani nacionalnih organov se uporablja Uredba (EU) 2016/679, razen če tako obdelavo izvajajo imenovani organi ali centralne točke dostopa držav članic za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj.
- (54) Kadar obdelavo osebnih podatkov v državah članicah za namen interoperabilnosti na podlagi te Uredbe izvajajo pristojni organi za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, se uporablja Direktiva (EU) 2016/680.
- (55) Uredba (EU) 2016/679, Uredba (EU) 2018/1725 ali, kadar je ustrezno, Direktiva (EU) 2016/680 se uporablja za vsak prenos osebnih podatkov v tretje države ali mednarodne organizacije, ki se izvede na podlagi te uredbe. Brez poseganja v razloge za prenos v skladu s poglavjem V Uredbe (EU) 2016/679 ali, kadar je to ustrezno, Direktivo (EU) 2016/680, se lahko kakršna koli sodba sodišča in odločba upravnega organa tretje države, ki od upravljavca ali obdelovalca zahteva prenos ali razkritje osebnih podatkov, prizna ali izvrši na kateri koli način le, če temelji na veljavnem mednarodnem sporazumu med tretjo državo prosilko in Unijo ali državo članico.
- (56) Za obdelavo osebnih podatkov v sistemih, katere urejata Uredba (EU) 2018/1862 in Uredba (EU) 2019/816 Evropskega parlamenta in Sveta <sup>(11)</sup> se uporabljajo posebne določbe o varstvu podatkov iz navedenih uredb.
- (57) Za obdelavo osebnih podatkov s strani eu-LISA ter drugih institucij in organov Unije zaradi izpolnjevanja njihovih obveznosti na podlagi te uredbe se uporablja Uredba (EU) 2018/1725, in sicer brez poseganja v Uredbo (EU) 2016/794, ki se uporablja za obdelavo osebnih podatkov s strani Europol.
- (58) Nadzorni organi iz Uredbe (EU) 2016/679 ali Direktive (EU) 2016/680, bi morali spremljati zakonitost obdelave osebnih podatkov s strani držav članic. Evropski nadzornik za varstvo podatkov bi moral spremljati dejavnosti institucij in organov Unije v zvezi z obdelavo osebnih podatkov. Evropski nadzornik za varstvo podatkov in nadzorni organi bi morali medsebojno sodelovati pri spremljanju obdelave osebnih podatkov prek sestavnih delov interoperabilnosti. Da lahko evropski nadzornik za varstvo podatkov izpolni naloge, ki so mu zaupane na podlagi te uredbe, so potrebni zadostni viri, vključno s človeškimi in finančnimi viri.
- (59) Opravljeno je bilo posvetovanje z Evropskim nadzornikom za varstvo podatkov v skladu s členom 28(2) Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta <sup>(12)</sup>, ki je mnenje podal 16. aprila 2018 <sup>(13)</sup>.
- (60) Delovna skupina za varstvo podatkov iz člena 29 je podala mnenje 11. aprila 2018.
- (61) Države članice in eu-LISA bi morale imeti varnostne načrte za lažje izpolnjevanje varnostnih obveznosti in bi morale medsebojno sodelovati, da bi obravnavale varnostna vprašanja. eu-LISA bi morala tudi zagotoviti stalno uporabo najnovejših tehnoloških inovacij, da bi se zagotovila celovitost podatkov v okviru razvoja, zasnove in upravljanja sestavnih delov interoperabilnosti. Obveznosti eu-LISA v zvezi s tem bi morale vključevati sprejetje

<sup>(11)</sup> Uredba (EU) 2019/816 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o vzpostavitvi centraliziranega sistema za določitev držav članic, ki imajo informacije o obsodbah državljanov tretjih držav in oseb brez državljanstva (sistem ECRIS-TCN) z namenom dopolnitve evropskega informacijskega sistema kazenskih evidenc ter o spremembi Uredbe (EU) 2018/1726 (glej stran 1 tega Uradnega lista).

<sup>(12)</sup> Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

<sup>(13)</sup> UL C 233, 4.7.2018, str. 12.

ukrepov, potrebnih za preprečevanje dostopa nepooblaščenih oseb, kot je osebje zunanjih ponudnikov storitev, do osebnih podatkov, ki se obdelujejo prek sestavnih delov interoperabilnosti. Pri sklepanju pogodb za zagotavljanje storitev bi morale države članice in eu-LISA upoštevati vse ukrepe, potrebne za zagotovitev skladnosti z zakoni ali predpisi v zvezi z varstvom osebnih podatkov in zasebnosti posameznikov ali za zaščito bistvenih varnostnih interesov, v skladu z Uredbo (EU) 2018/1046 Evropskega parlamenta in Sveta <sup>(14)</sup> ter veljavnimi mednarodnimi konvencijami. eu-LISA bi morala upoštevati načeli vgrajene in privzete zasebnosti v fazi razvoja sestavnih delov interoperabilnosti.

- (62) Za statistične namene in namene poročanja je treba pooblaščenemu osebju pristojnih organov, institucij in agencij Unije iz te uredbe odobriti dostop do nekaterih podatkov v zvezi z nekaterimi sestavnimi deli interoperabilnosti, ne da bi se omogočila identifikacija posameznikov.
- (63) Da bi se lahko organi držav članic in agencije Unije prilagodili novim zahtevam glede uporabe ESP, je treba zagotoviti prehodno obdobje. Podobno bi bilo treba za skladno in optimalno delovanje MID določiti prehodne ukrepe za začetek njegovega delovanja.
- (64) Ker cilja te uredbe, in sicer vzpostavitev okvira za interoperabilnost informacijskih sistemov EU, države članice ne morejo zadovoljivo doseči, temveč se zaradi obsega in učinkov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji (PEU). V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseg navedenega cilja.
- (65) Preostali znesek v proračunu, določen za pametne meje v Uredbi (EU) št. 515/2014 Evropskega parlamenta in Sveta <sup>(15)</sup> bi bilo treba prerazporediti za to uredbo v skladu s členom 5(5)(b) Uredbe (EU) št. 515/2014, da pokrije stroške za razvoj sestavnih delov interoperabilnosti.
- (66) Za dopolnitev nekaterih podrobnih tehničnih vidikov te uredbe bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 Pogodbe o delovanju Evropske unije (PDEU) sprejme akte glede:

- podaljšanja prehodnega obdobja za uporabo ESP,
- podaljšanja prehodnega obdobja za ugotavljanje več identitet, ki ga izvede centralna enota ETIAS,
- postopkov za odkrivanje primerov, v katerih se lahko podatki o identiteti štejejo za enake ali podobne,
- pravil o delovanju CRRS, vključno s specifičnimi zaščitnimi ukrepi za obdelavo osebnih podatkov ter varnostnih pravil, ki veljajo za register, in
- podrobnih pravil o delovanju spletnega portala.

Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, vključno na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje <sup>(16)</sup>. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njunim strokovnjakom pa se sistematično lahko udeležijo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

- (67) Za zagotovitev enotnih pogojev izvajanja te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila za določitev datumov začetka delovanja ESP, skupne BMS, CIR, MID in CRRS.

<sup>(14)</sup> Uredba (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije, spremembi uredb (EU) št. 1296/2013, (EU) št. 1301/2013, (EU) št. 1303/2013, (EU) št. 1304/2013, (EU) št. 1309/2013, (EU) št. 1316/2013, (EU) št. 223/2014, (EU) št. 283/2014 in Sklepa št. 541/2014/EU ter razveljavitvi Uredbe (EU, Euratom) št. 966/2012 (UL L 193, 30.7.2018, str. 1).

<sup>(15)</sup> Uredba (EU) št. 515/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o vzpostavitvi instrumenta za finančno podporo na področju zunanjih meja in vizumov v okviru Sklada za notranjo varnost in o razveljavitvi Odločbe št. 574/2007/ES (UL L 150, 20.5.2014, str. 143).

<sup>(16)</sup> UL L 123, 12.5.2016, str. 1.

- (68) Na Komisijo bi bilo treba prenesti tudi izvedbena pooblastila v zvezi s sprejetjem podrobnih pravil o: tehničnih podrobnostih profilov uporabnikov ESP; podrobnostih tehnične rešitve za omogočanje poizvedovanja prek ESP v informacijskih sistemih EU, podatkih Europol in Interpolovih podatkovnih zbirkah, ter formatu odgovorov prek ESP; tehničnih pravilih za ustvarjanje povezav v MID med podatki iz različnih informacijskih sistemov EU; vsebini in obliki obrazca za obveščanje posameznika, na katerega se nanašajo osebni podatki, če se vzpostavi rdeča povezava; zahtevah glede učinkovitosti in spremljanja učinkovitosti skupne BMS; samodejnih mehanizmi, postopkih in kazalnikov za nadzor kakovosti podatkov; razvoju standarda UMF; postopku sodelovanja v primeru varnostnega incidenta; in specifikacijah tehnične rešitve za države članice za upravljanje zahtev za dostop uporabnikov. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta <sup>(17)</sup>.
- (69) Ker bodo sestavni deli interoperabilnosti vključevali obdelavo velikih količin občutljivih osebnih podatkov, je pomembno, da lahko osebe, katerih osebni podatki se obdelujejo z uporabo teh sestavnih delov, učinkovito uresničujejo svoje pravice kot posamezniki, na katere se nanašajo osebni podatki, kot se zahteva na podlagi Uredbe (EU) 2016/679, Direktive (EU) 2016/680 in Uredbe (EU) 2018/1725. Posameznikom, na katere se nanašajo osebni podatki, bi bilo treba zagotoviti spletni portal, ki bi jim olajšal uveljavljanje pravic dostopa ter popravka, izbrisa in omejitve obdelave svojih osebnih podatkov. eu-LISA bi morala vzpostaviti in upravljati tak spletni portal.
- (70) Eno izmed glavnih načel varstva podatkov je najmanjši obseg podatkov: v skladu s členom 5(1)(c) Uredbe (EU) 2016/679 mora biti obdelava osebnih podatkov ustrezna, relevantna in omejena na to, kar je potrebno za namene, za katere se obdelujejo. Zato sestavni deli interoperabilnosti ne bi smeli omogočati shranjevanja nobenih novih osebnih podatkov, razen povezav, ki bodo shranjene v MID in so najmanj, kar je potrebno za namene te uredbe.
- (71) Ta uredba bi morala vsebovati jasne določbe o odgovornosti in pravici do odškodnine zaradi nezakonite obdelave osebnih podatkov ali katerega koli drugega dejanja, ki je nezdružljiv s to uredbo. Take določbe ne bi smele posegati v pravico do odškodnine od upravljavca ali obdelovalca in v njuno odgovornost na podlagi Uredbe (EU) 2016/679, Direktive (EU) 2016/680 in Uredbe (EU) 2018/1725. eu-LISA bi morala biti v vlogi obdelovalca podatkov odgovorna za morebitno škodo, ki bi nastala, kadar ni izpolnjevanja obveznosti, ki so ji konkretno naložene s to uredbo, ali kadar je prekoračila zakonita navodila države članice, ki je upravljavec podatkov, oziroma ravnala v nasprotju z njimi.
- (72) Ta uredba ne posega v uporabo Direktive 2004/38/ES Evropskega parlamenta in Sveta <sup>(18)</sup>.
- (73) V skladu s členoma 1 in 2 Protokola št. 22 o stališču Danske, ki je priložen PEU in PDEU, Danska ne sodeluje pri sprejetju te uredbe, ki zato zanjo ni zavezujoča in se v njej ne uporablja. Ker ta uredba, kolikor se njene določbe nanašajo na SIS, kakor ga ureja Uredba (EU) 2018/1862, nadgrajuje schengenski pravni red, se Danska v skladu s členom 4 navedenega protokola v šestih mesecih od dne, ko Svet sprejme to uredbo, odloči, ali jo bo prenesla v svoje nacionalno pravo.
- (74) Kolikor se njene določbe nanašajo na SIS, kakor ga ureja Uredba (EU) 2018/1862, Združeno kraljestvo sodeluje pri tej uredbi v skladu s členom 5(1) Protokola št. 19 o schengenskem pravnem redu, vključenem v okvir Evropske unije, ki je priložen PEU in PDEU, in členom 8(2) Sklepa Sveta 2000/365/ES <sup>(19)</sup>. Poleg tega, kolikor se njene določbe nanašajo na sistem Eurodac in sistem ECRIS-TCN, je Združeno kraljestvo v pismu z dne 18. maja 2018 podalo uradno obvestilo, da želi sodelovati pri sprejetju in uporabi te uredbe v skladu s členom 3 Protokola št. 21 o stališču Združenega kraljestva in Irske glede območja svobode, varnosti in pravice, priloženega PEU in PDEU.

<sup>(17)</sup> Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13).

<sup>(18)</sup> Direktiva Evropskega parlamenta in Sveta 2004/38/ES z dne 29. aprila 2004 o pravici državljanov Unije in njihovih družinskih članov do prostega gibanja in prebivanja na ozemlju držav članic, ki spreminja Uredbo (EGS) št. 1612/68 in razveljavlja Direktive 64/221/EGS, 68/360/EGS, 72/194/EGS, 73/148/EGS, 75/34/EGS, 75/35/EGS, 90/364/EGS, 90/365/EGS in 93/96/EGS (UL L 158, 30.4.2004, str. 77).

<sup>(19)</sup> Sklep Sveta 2000/365/ES z dne 29. maja 2000 o prošnji Združenega kraljestva Velike Britanije in Severne Irske za sodelovanje pri izvajanju nekaterih določb schengenskega pravnega reda (UL L 131, 1.6.2000, str. 43).

- (75) Kolikor se njene določbe nanašajo na SIS, kakor ga ureja Uredba (EU) 2018/1862, bi lahko Irska načeloma sodelovala pri tej uredbi v skladu s členom 5(1) Protokola št. 19 o schengenskem pravnem redu, vključenem v okvir Evropske unije, ki je priložen PEU in PDEU, in členom 6(2) Sklepa Sveta 2002/192/ES <sup>(20)</sup>. Poleg tega, kolikor se njene določbe nanašajo na sistem Eurodac in sistem ECRIS-TCN, Irska v skladu s členoma 1 in 2 Protokola št. 21 o stališču Združenega kraljestva in Irske glede območja svobode, varnosti in pravice, priloženega PEU in PDEU, in brez poseganja v člen 4 navedenega protokola, ne sodeluje pri sprejetju te uredbe, ki zato zanj ni zavezujoča in se v njej ne uporablja. Ker v danih okoliščinah ni mogoče zagotoviti, da se ta uredba v celoti uporablja za Irsko, ko je določeno v členu 288 PDEU, Irska, brez poseganja v njene pravice na podlagi protokolov št. 19 in št. 21, ne sodeluje pri sprejetju te uredbe, ki zato zanj ni zavezujoča in se v njej ne uporablja.
- (76) Ta uredba, kolikor zadeva SIS, kakor ga ureja Uredba (EU) 2018/1862, za Islandijo in Norveško predstavlja razvoj določb schengenskega pravnega reda v smislu Sporazuma med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško o pridružitvi obeh k izvajanju, uporabi in razvoju schengenskega pravnega reda <sup>(21)</sup>, ki spadajo na področje iz točke G člena 1 Sklepa Sveta 1999/437/ES <sup>(22)</sup>.
- (77) Ta uredba, kolikor zadeva SIS, kakor ga ureja Uredba (EU) 2018/1862, za Švico predstavlja razvoj določb schengenskega pravnega reda v smislu Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda <sup>(23)</sup>, ki spadajo na področje iz točke G člena 1 Sklepa Sveta 1999/437/ES v povezavi s členom 3 Sklepa Sveta 2008/149/PNZ <sup>(24)</sup>.
- (78) Ta uredba, kolikor zadeva SIS, kakor ga ureja Uredba (EU) 2018/1862, za Lihtenštajn predstavlja razvoj določb schengenskega pravnega reda v smislu Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda <sup>(25)</sup>, ki spadajo na področje iz točke G člena 1 Sklepa Sveta 1999/437/ES v povezavi s členom 3 Sklepa Sveta 2011/350/EU <sup>(26)</sup>.
- (79) Ta uredba spoštuje temeljne pravice in upošteva načela, ki jih priznava zlasti Listina Evropske unije o temeljnih pravicah, ter bi se morala uporabljati v skladu s temi pravicami in načeli.
- (80) Da bi bila ta uredba v skladu z obstoječim pravnim okvirom, bi bilo treba ustrezno spremeniti Uredbo (EU) 2018/1726 Evropskega parlamenta in Sveta <sup>(27)</sup> ter uredbi (EU) 2018/1862 in (EU) 2019/816 –

<sup>(20)</sup> Sklep Sveta 2002/192/ES z dne 28. februarja 2002 o prošnji Irske, da sodeluje pri izvajanju nekaterih določb schengenskega pravnega reda (UL L 64, 7.3.2002, str. 20).

<sup>(21)</sup> UL L 176, 10.7.1999, str. 36.

<sup>(22)</sup> Sklep Sveta 1999/437/ES z dne 17. maja 1999 o nekaterih izvedbenih predpisih za uporabo Sporazuma, sklenjenega med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško, v zvezi s pridružitvijo teh dveh držav k izvajanju, uporabi in razvoju schengenskega pravnega reda (UL L 176, 10.7.1999, str. 31).

<sup>(23)</sup> UL L 53, 27.2.2008, str. 52.

<sup>(24)</sup> Sklep Sveta 2008/149/PNZ z dne 28. januarja 2008 o sklenitvi Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda v imenu Evropske unije (UL L 53, 27.2.2008, str. 50).

<sup>(25)</sup> UL L 160, 18.6.2011, str. 21.

<sup>(26)</sup> Sklep Sveta 2011/350/EU z dne 7. marca 2011 o sklenitvi Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda, v zvezi z odpravo kontrol na notranjih mejah in prostim gibanjem oseb, v imenu Evropske unije (UL L 160, 18.6.2011, str. 19).

<sup>(27)</sup> Uredba (EU) 2018/1726 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o Agenciji Evropske unije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (eu-LISA), o spremembi Uredbe (ES) št. 1987/2006 in Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (EU) št. 1077/2011 (UL L 295, 21.11.2018, str. 99).

SPREJELA NASLEDNJO UREDBO:

## POGLAVJE I

### Splošne določbe

#### Člen 1

#### Predmet urejanja

1. Ta uredba skupaj z Uredbo (EU) 2019/817 Evropskega parlamenta in Sveta <sup>(28)</sup> vzpostavlja okvir za zagotovitev interoperabilnosti sistema vstopa/izstopa (SVI), vizumskega informacijskega sistema (VIS), evropskega sistema za potovalne informacije in odobritve (ETIAS), sistema Eurodac, schengenskega informacijskega sistema (SIS) in evropskega informacijskega sistema kazenskih evidenc za državljane tretjih držav (v nadaljnjem besedilu: sistem ECRIS-TCN).
2. Okvir vsebuje naslednje sestavne dele interoperabilnosti:
  - (a) evropski iskalni portal (ESP);
  - (b) skupno storitev za ugotavljanje ujemanja biometričnih podatkov (v nadaljnjem besedilu: skupna BMS);
  - (c) skupno odložišče podatkov o identiteti (CIR);
  - (d) detektor več identitet (MID).
3. Ta uredba vsebuje tudi določbe o zahtevah glede kakovosti podatkov, univerzalnem formatu sporočil (UMF) in centralnem registru za poročanje in statistične podatke (CRRS) ter o pristojnostih držav članic in Evropske agencije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (eu-LISA) v zvezi z zasnovo, razvojem in delovanjem sestavnih delov interoperabilnosti.
4. Ta uredba tudi prilagaja postopke in pogoje za dostop imenovanih organov in Agencije Evropske unije za sodelovanje na področju kazenskega pregona (Europol) do SVI, VIS, ETIAS in sistema Eurodac za namene preprečevanja, odkrivanja in preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj.
5. Ta uredba določa tudi okvir za preverjanje identitete oseb in za identifikacijo oseb.

#### Člen 2

#### Cilji

1. Cilji te uredbe so z zagotavljanjem interoperabilnosti:
  - (a) izboljšati učinkovitost in uspešnost mejnih kontrol na zunanjih mejah;
  - (b) prispevati k preprečevanju nezakonitega priseljevanja in boju proti njemu;
  - (c) prispevati k visoki ravni varnosti na območju svobode, varnosti in pravice v Uniji, vključno z vzdrževanjem javne varnosti in javnega reda ter zagotavljanjem varnosti na ozemljih držav članic;
  - (d) izboljšati izvajanje skupne vizumske politike;
  - (e) pomagati pri obravnavi prošenj za mednarodno zaščito;
  - (f) prispevati k preprečevanju, odkrivanju in preiskovanju terorističnih kaznivih dejanj in drugih hudih kaznivih dejanj;
  - (g) olajšati identifikacijo neznanih oseb, ki se ne morejo same identificirati, ali neidentificiranih človeških ostankov v primeru naravne nesreče, nezgode ali terorističnega napada.
2. Cilji iz odstavka 1 se dosežejo z:
  - (a) zagotavljanjem pravilne identifikacije oseb;
  - (b) prispevanjem k boju proti identitetnim prevaram;

<sup>(28)</sup> Uredba (EU) 2019/817 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju meja in vizumov ter spremembi uredb (ES) št. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 in (EU) 2018/1861 Evropskega parlamenta in Sveta ter Odločbe Sveta 2004/512/ES in Sklepa Sveta 2008/633/PNZ (glej stran 27 tega Uradnega lista).

- (c) izboljšanjem kakovosti podatkov in uskladitvijo zahtev glede kakovosti podatkov, hranjenih v informacijskih sistemih EU, ob spoštovanju zahtev pravnih instrumentov, ki urejajo posamezne sisteme, glede obdelovanja podatkov ter standardov in načel za varstvo podatkov;
- (d) olajšanjem in podpiranjem tehničnega in operativnega izvajanja informacijskih sistemov EU s strani držav članic;
- (e) krepitvijo, poenostavitvijo in uskladitvijo pogojev za varnost in varstvo podatkov, ki urejajo zadevne informacijske sisteme EU, brez vpliva na posebne zaščitne in varnostne ukrepe, ki se uporabljajo za nekatere kategorije podatkov;
- (f) racionalizacijo pogojev za dostop imenovanih organov do SVI, VIS, ETIAS in sistema Eurodac ob hkratnem zagotavljanju potrebnih in sorazmernih pogojev za ta dostop;
- (g) podpiranjem namenov SVI, VIS, ETIAS, sistema Eurodac, SIS in sistema ECRIS-TCN.

### Člen 3

#### Področje uporabe

1. Ta uredba se uporablja za sistem Eurodac, SIS in sistem ECRIS-TCN.
2. Ta uredba se uporablja tudi za podatke Europol v obsegu, ki omogoča sočasno poizvedovanje po njih in po informacijskih sistemih EU iz odstavka 1.
3. Ta uredba se uporablja za osebe, katerih osebni podatki se lahko obdelujejo v informacijskih sistemih EU iz odstavka 1 in v podatkih Europol iz odstavka 2.

### Člen 4

#### Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

- (1) „zunanje meje“ pomeni zunanje meje, kakor so opredeljene v točki 2 člena 2 Uredbe (EU) 2016/399 Evropskega parlamenta in Sveta <sup>(29)</sup>;
- (2) „mejna kontrola“ pomeni mejno kontrolo, kakor je opredeljena v točki 11 člena 2 Uredbe (EU) 2016/399;
- (3) „mejni organ“ pomeni mejnega policista, ki v skladu z nacionalno zakonodajo izvaja mejno kontrolo;
- (4) „nadzorni organi“ pomeni nadzorni organ iz člena 51(1) Uredbe (EU) 2016/679, in nadzorni organ iz člena 41(1) Direktive (EU) 2016/680;
- (5) „preverjanje“ pomeni postopek primerjave nizov podatkov zaradi potrjevanja zatrjevanje identitete (preverjanje s primerjanjem z enim vzorcem);
- (6) „identifikacija“ pomeni postopek ugotavljanja identitete osebe s primerjanjem več nizov podatkov v podatkovni zbirki (preverjanje s primerjanjem z več vzorci);
- (7) „alfanumerični podatki“ pomeni podatke, ki so predstavljeni s črkami, številkami, posebnimi znaki, razmiki med znaki in ločili;
- (8) „podatki o identiteti“ pomeni podatke iz člena 27(3)(a) do (e);
- (9) „podatki o prstnih odtisih“ pomeni slike prstnih odtisov in sledi prstnih odtisov, ki zaradi svojih edinstvenih značilnosti in vsebovanih referenčnih točk omogočajo točno in jasno primerjavo identitete osebe;

<sup>(29)</sup> Uredba (EU) 2016/399 Evropskega parlamenta in Sveta z dne 9. marca 2016 o Zakoniku Unije o pravilih, ki urejajo gibanje oseb prek meja (Zakonik o schengenskih mejah) (UL L 77, 23.3.2016, str. 1).

- (10) „podoba obraza“ pomeni digitalne slike obraza;
- (11) „biometrični podatki“ pomeni podatke o prstnih odtisih ali podobe obraza ali oboje;
- (12) „biometrična predloga“ pomeni matematično predstavitev, ki je pridobljena z ekstrakcijo značilnosti iz biometričnih podatkov in omejena na značilnosti, potrebne za identifikacijo in preverjanje;
- (13) „potna listina“ pomeni potni list ali drug enakovreden dokument, s katerim je imetnik upravičen do prehoda zunanjih meja in v katerega se lahko pritrdi vizum;
- (14) „podatki o potni listini“ pomeni vrsto, številko in državo izdajateljico potne listine, datum izteka njene veljavnosti in tričrkovno oznako države izdajateljice;
- (15) „informacijski sistemi EU“ pomeni SVI, VIS, ETIAS, sistem Eurodac, SIS in sistem ECRIS-TCN;
- (16) „podatki Europol“ pomeni osebne podatke, ki jih obdela Europol za namen iz člena 18(2)(a), (b) in (c) Uredbe (EU) 2016/794;
- (17) „Interpolovi podatkovni zbirki“ pomeni Interpolovo podatkovno zbirko o ukradenih in izgubljenih potovalnih dokumentih (v nadaljnjem besedilu: podatkovna zbirka SLTD) ter Interpolovo zbirko potovalnih dokumentov, povezanih z razpisi ukrepov (v nadaljnjem besedilu: podatkovna zbirka TDAWN);
- (18) „ujemanje“ pomeni obstoj povezave, ugotovljene s samodejno primerjavo osebnih podatkov, ki so evidentirani ali se evidentirajo v informacijskem sistemu ali podatkovni zbirki;
- (19) „policijski organ“ pomeni pristojni organ, kakor je opredeljen v točki 7 člena 3 Direktive (EU) 2016/680;
- (20) „imenovani organi“ pomeni imenovane organe držav članic, kot so opredeljeni v točki 26 člena 3 Uredbe (EU) 2017/2226 Evropskega parlamenta in Sveta <sup>(30)</sup>, točki (e) člena 2(1) Sklepa Sveta 2008/633/PNZ <sup>(31)</sup> in točki 21 člena 3(1) Uredbe (EU) 2018/1240 Evropskega parlamenta in Sveta <sup>(32)</sup>;
- (21) „teroristično kaznivo dejanje“ pomeni kaznivo dejanje po nacionalnem pravu, ki ustreza ali je enakovredno enemu izmed kaznivih dejanj iz Direktive (EU) 2017/541 Evropskega parlamenta in Sveta <sup>(33)</sup>;
- (22) „hudo kaznivo dejanje“ pomeni kaznivo dejanje, ki ustreza ali je enakovredno enemu izmed kaznivih dejanj iz člena 2(2) Okvirnega Sklepa Sveta 2002/584/PNZ <sup>(34)</sup>, če se po nacionalnem pravu kaznuje z zaporno kaznijo ali ukrepom odvzema prostosti z najvišjo zagroženo kaznijo najmanj treh let;
- (23) „sistem vstopa/izstopa“ ali „SVI“ pomeni sistem vstopa/izstopa, vzpostavljen z Uredbo (EU) 2017/2226;
- (24) „vizumski informacijski sistem“ ali „VIS“ pomeni vizumski informacijski sistem, vzpostavljen z Uredbo (ES) št. 767/2008 Evropskega parlamenta in Sveta <sup>(35)</sup>;
- (25) „evropski sistem za potovalne informacije in odobritve“ ali „ETIAS“ pomeni evropski sistem za potovalne informacije in odobritve, vzpostavljen z Uredbo (EU) 2018/1240;

<sup>(30)</sup> Uredba (EU) 2017/2226 Evropskega parlamenta in Sveta z dne 30. novembra 2017 o vzpostavitvi sistema vstopa/izstopa (SVI) za evidentiranje podatkov o vstopu in izstopu ter podatkov o zavrnitvi vstopa državljanov tretjih držav pri prehajanju zunanjih meja držav članic in določiti pogojev za dostop do SVI zaradi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter o spremembi Konvencije o izvajanju Schengenskega sporazuma in uredb (ES) št. 767/2008 ter (EU) št. 1077/2011 (UL L 327, 9.12.2017, str. 20).

<sup>(31)</sup> Sklep Sveta 2008/633/PNZ z dne 23. junija 2008 o dostopu imenovanih organov držav članic in Europol do vizumskega informacijskega sistema (VIS) za iskanje podatkov za namene preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj (UL L 218, 13.8.2008, str. 129).

<sup>(32)</sup> Uredba (EU) 2018/1240 Evropskega parlamenta in Sveta z dne 12. septembra 2018 o vzpostavitvi Evropskega sistema za potovalne informacije in odobritve (ETIAS) ter spremembi uredb (EU) št. 1077/2011, (EU) št. 515/2014, (EU) 2016/399, (EU) 2016/1624 in (EU) 2017/2226 (UL L 236, 19.9.2018, str. 1).

<sup>(33)</sup> Direktiva (EU) 2017/541 Evropskega parlamenta in Sveta z dne 15. marca 2017 o boju proti terorizmu in nadomestitvi Okvirnega sklepa Sveta 2002/475/PNZ ter o spremembi Sklepa Sveta 2005/671/PNZ (UL L 88, 31.3.2017, str. 6).

<sup>(34)</sup> Okvirni sklep Sveta 2002/584/PNZ z dne 13. junija 2002 o Evropskem nalogu za prijetje in postopkih predaje med državami članicami (UL L 190, 18.7.2002, str. 1).

<sup>(35)</sup> Uredba (ES) št. 767/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje (Uredba VIS) (UL L 218, 13.8.2008, str. 60).

- (26) „sistem Eurodac“ pomeni sistem Eurodac, vzpostavljen z Uredbo (EU) št. 603/2013 Evropskega parlamenta in Sveta <sup>(36)</sup>;
- (27) „schengenski informacijski sistem“ ali „SIS“ pomeni schengenski informacijski sistem, vzpostavljen z uredbami (EU) 2018/1860, (EU) 2018/1861 in (EU) 2018/1862;
- (28) „sistem ECRIS-TCN“ pomeni centralizirani sistem za določitev držav članic, ki hranijo informacije o obsodbah državljanov tretjih držav in oseb brez državljanstva, vzpostavljen z Uredbo (EU) 2019/816.

## Člen 5

### Nediskriminacija in temeljne pravice

Obdelava osebnih podatkov za namene te uredbe ne sme povzročiti diskriminacije oseb na kakršni koli podlagi, kot so spol, rasa, barva kože, etnično ali družbeno poreklo, genetske značilnosti, jezik, vera ali prepričanje, politično ali kakršno koli drugo stališče, pripadnost narodni manjšini, premoženje, rojstvo, invalidnost, starost ali spolna usmerjenost. V celoti mora spoštovati človekovo dostojanstvo in integriteto ter temeljne pravice, vključno s pravico do spoštovanja zasebnega življenja in pravico do varstva osebnih podatkov. Posebna pozornost se nameni otrokom, starejšim osebam, invalidom ter osebam, ki potrebujejo mednarodno zaščito. Največja korist otroka je najpomembnejše vodilo.

## POGLAVJE II

### Evropski iskalni portal

## Člen 6

### Evropski iskalni portal

1. Evropski iskalni portal (ESP) se vzpostavi za namene spodbujanja hitrega, nemotenega, učinkovitega, sistematičnega in nadzorovanega dostopa organov držav članic in agencij Unije do informacijskih sistemov EU, podatkov Europol in Interpolovih podatkovnih zbirk za opravljanje njihovih nalog in v skladu s pravicami do dostopa ter cilji in nameni SVI, VIS, ETIAS, sistema Eurodac, SIS in sistema ECRIS-TCN.
2. ESP sestavljajo:
  - (a) centralna infrastruktura, vključno z iskalnim portalom, ki omogoča sočasno iskanje v SVI, VIS, ETIAS, sistemu Eurodac, SIS, sistemu ECRIS-TCN, po podatkih Europol in v Interpolovih podatkovnih zbirkah;
  - (b) varen komunikacijski kanal med ESP, državami članicami in agencijami Unije, ki so upravičene do uporabe ESP;
  - (c) varna komunikacijska infrastruktura med ESP in SVI, VIS, ETIAS, sistemom Eurodac, centralnim SIS, sistemom ECRIS-TCN, podatki Europol in Interpolovima podatkovnima zbirkama ter med ESP in centralno infrastrukturo CIR in MID.
3. ESP razvija in tehnično upravlja eu-LISA.

## Člen 7

### Uporaba evropskega iskalnega portala

1. Uporaba ESP je omejena na organe držav članic in agencije Unije, ki imajo dostop vsaj do enega od informacijskih sistemov EU v skladu s pravnimi instrumenti, ki urejajo te informacijske sisteme EU, do CIR in MID v skladu s to uredbo ter do podatkov Europol v skladu z Uredbo (EU) 2016/794 ali do Interpolovih podatkovnih zbirk v skladu s pravom Unije ali nacionalnim pravom, ki ureja tak dostop.

Ti organi držav članic in agencije Unije lahko uporabljajo ESP in podatke, ki jih zagotavlja, le za cilje in namene, določene v pravnih instrumentih, ki urejajo te informacijske sisteme EU, v Uredbi (EU) 2016/794 in v tej uredbi.

<sup>(36)</sup> Uredba (EU) št. 603/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o vzpostavitvi sistema Eurodac za primerjavo prstnih odtisov zaradi učinkovite uporabe Uredbe (EU) št. 604/2013 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vloži državljan tretje države ali oseba brez državljanstva, in o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona, ter o spremembi Uredbe (EU) št. 1077/2011 o ustanovitvi Evropske agencije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (UL L 180, 29.6.2013, str. 1).

2. Organi držav članic in agencije Unije iz odstavka 1 uporabljajo ESP za iskanje podatkov, ki se nanašajo na osebe ali njihove potne listine, v centralnih sistemih sistema Eurodac in sistema ECRIS-TCN v skladu s pravicami dostopa, določenimi v pravnih instrumentih, ki urejajo te informacijske sisteme EU, in v nacionalnem pravu. Uporabljajo ga tudi za poizvedovanje v CIR v skladu s pravicami dostopa po tej uredbi za namene iz členov 20, 21 in 22.
3. Organi držav članic iz odstavka 1 lahko uporabljajo ESP za iskanje podatkov, ki se nanašajo na osebe ali njihove potne listine, v centralnem SIS iz uredb (EU) 2018/1860 in (EU) 2018/1861.
4. Kadar tako določa pravo Unije, agencije Unije iz odstavka 1 uporabljajo ESP za iskanje podatkov, ki se nanašajo na osebe ali njihove potne listine, v centralnem SIS.
5. Organi držav članic in agencije Unije iz odstavka 1 lahko uporabljajo ESP za iskanje podatkov, ki se nanašajo na osebe ali njihove potne listine, v podatkih Europol v skladu s pravicami dostopa po pravu Unije in nacionalnem pravu.

## Člen 8

### Profili uporabnikov evropskega iskalnega portala

1. Da se omogoči uporaba ESP, eu-LISA v sodelovanju z državami članicami ustvari profil na podlagi vsake kategorije uporabnika ESP in namenov poizvedb v skladu s tehničnimi podrobnostmi in pravicami dostopa iz odstavka 2. Vsak profil v skladu s pravom Unije in nacionalnim pravom vsebuje naslednje informacije:
  - (a) podatkovna polja, ki se uporabljajo za poizvedovanje;
  - (b) informacijske sisteme EU, podatke Europol in Interpolovi podatkovni zbirki, v katerih se in se lahko poizveduje ter tiste, ki morajo zagotoviti odgovor uporabniku;
  - (c) konkretne podatke v informacijskih sistemih EU, podatkih Europol in Interpolovih podatkovnih zbirkah, v katerih se lahko poizveduje;
  - (d) kategorije podatkov, ki se lahko navedejo v posameznem odgovoru.
2. Komisija sprejme izvedbene akte za določitev tehničnih podrobnosti profilov iz odstavka 1 v skladu s pravicami dostopa uporabnikov ESP na podlagi pravnih instrumentov, ki urejajo informacijske sisteme EU, in na podlagi nacionalnega prava. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 70(2).
3. eu-LISA v sodelovanju redno, najmanj pa enkrat letno, pregleduje profile iz odstavka 1 in jih po potrebi posodobi.

## Člen 9

### Poizvedbe

1. Uporabniki ESP sprožijo poizvedbo z vnosom alfanumeričnih in/ali biometričnih podatkov v ESP. Kadar je sprožena poizvedba, ESP s podatki, ki jih vnese uporabnik ESP, v skladu z uporabniškim profilom sočasno poizveduje v SVI, ETIAS, VIS, SIS, sistemu Eurodac, sistemu ECRIS-TCN, CIR, po podatkih Europol in v Interpolovih podatkovnih zbirkah.
2. Kategorije podatkov, ki se uporabijo za sprožitev poizvedbe prek ESP, ustrezajo kategorijam podatkov, ki se nanašajo na osebe ali potne listine in se lahko uporabijo za poizvedovanje v različnih informacijskih sistemih EU, po podatkih Europol in v Interpolovih podatkovnih zbirkah v skladu s pravnimi instrumenti, ki jih urejajo.
3. eu-LISA v sodelovanju z državami članicami za ESP uvede kontrolni dokument vmesnika, ki temelji na UMF iz člena 38.
4. Kadar uporabnik ESP sproži poizvedbo, se v odgovor na poizvedbo zagotovijo podatki, ki jih vsebujejo SVI, ETIAS, VIS, SIS, sistem Eurodac, sistem ECRIS-TCN, CIR, MID, podatki Europol in Interpolovi podatkovni zbirki.

Brez poseganja v člen 20 se v odgovoru, ki ga zagotovi ESP, navede, kateremu informacijskemu sistemu ali podatkovni zbirki EU podatki pripadajo.

ESP ne zagotovi informacij o podatkih iz informacijskih sistemov EU, podatkov Europol in Interpolovih podatkovnih zbirk do katerih uporabnik na podlagi veljavnega prava Unije in nacionalnega prava nima dostopa.

5. Vsako poizvedovanje v Interpolovih podatkovnih zbirkah prek ESP se izvede tako, da se lastniku razpisa ukrepa Interpola ne razkrijejo nobene informacije.
6. ESP odgovor uporabniku zagotovi takoj, ko so na voljo podatki iz enega od informacijskih sistemov EU, podatkov Europol ali Interpolovih podatkovnih zbirk. Ti odgovori vsebujejo samo podatke, do katerih ima uporabnik dostop na podlagi prava Unije in nacionalnega prava.
7. Komisija sprejme izvedbeni akt, v katerem določi tehnični postopek, po katerem ESP poizveduje v informacijskih sistemih EU, podatkih Europol in Interpolovih podatkovnih zbirkah, ter format odgovorov prek ESP. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 70(2).

#### Člen 10

##### Vodenje dnevnikov

1. Brez poseganja v člena 12 in 18 Uredbe (EU) 2018/1862, člen 29 Uredbe (EU) 2019/816 ter člen 40 Uredbe (EU) 2016/794 agencija eu-LISA vodi dnevnike o vseh postopkih obdelave podatkov v ESP. Ti dnevniki vključujejo naslednje:
  - (a) organ države članice ali agencijo Unije, ki sproži poizvedbo, in uporabljeni profil ESP;
  - (b) datum in čas poizvedbe;
  - (c) poizvedovane informacijske sisteme EU in podatke Europol.
2. Vsaka država članica vodi dnevnike o poizvedbah, ki jih opravijo njeni organi in osebje teh organov, ki je pooblaščen za uporabo ESP. Vsaka agencija Unije vodi dnevnike o poizvedbah, ki jih opravi njeno pooblaščen osebje.
3. Dnevniki iz odstavkov 1 in 2 se lahko uporabljajo izključno za spremljanje varstva podatkov, vključno s preverjanjem dopustnosti poizvedbe in zakonitosti obdelave podatkov, in za zagotavljanje varnosti in celovitosti podatkov. Ti dnevniki se z ustreznimi ukrepi zaščitijo pred nepooblaščenim dostopom in izbrišejo po enem letu od njihovega nastanka. Če so dnevniki potrebni za že začete postopke spremljanja, se izbrišejo, ko niso več potrebni za postopke spremljanja.

#### Člen 11

##### Nadomestni postopki v primeru tehnične nezmožnosti uporabe evropskega iskalnega portala

1. Kadar je zaradi izpada delovanja ESP slednjega tehnično nemogoče uporabiti za poizvedovanje v enem ali več informacijskih sistemih EU ali CIR, eu-LISA o tem samodejno obvesti uporabnike ESP.
2. Kadar je zaradi izpada delovanja nacionalne infrastrukture v državi članici ESP tehnično nemogoče uporabiti za poizvedovanje v enem ali več informacijskih sistemih EU ali CIR, ta država članica o tem samodejno obvesti eu-LISA in Komisijo.
3. V primerih iz odstavka 1 ali 2 tega člena in do odprave tehnične okvare obveznosti iz člena 7(2) in (4) ne veljajo in države članice dostopajo do informacijskih sistemov EU ali CIR neposredno, kadar se to od njih zahteva na podlagi prava Unije ali nacionalnega prava.
4. Kadar je zaradi izpada delovanja infrastrukture agencije Unije tehnično nemogoče uporabiti ESP za poizvedovanje v enem ali več informacijskih sistemih EU ali CIR, ta agencija o tem samodejno obvesti eu-LISA in Komisijo.

#### POGLAVJE III

##### Skupna storitev za ugotavljanje ujemanja biometričnih podatkov

#### Člen 12

##### Skupna storitev za ugotavljanje ujemanja biometričnih podatkov

1. Za namene podpiranja CIR in MID ter ciljev SVI, VIS, sistema Eurodac, SIS in sistema ECRIS-TCN se vzpostavi skupna storitev za ugotavljanje ujemanja biometričnih podatkov (v nadaljnjem besedilu: skupna BMS), ki hrani biometrične predloge, pridobljene iz biometričnih podatkov iz člena 13, ki se hranijo v CIR in SIS, in omogoča poizvedovanje v več informacijskih sistemih EU na podlagi biometričnih podatkov.

2. Skupno BMS sestavljajo:
  - (a) centralna infrastruktura, ki nadomesti centralne sisteme SVI, VIS, SIS, sistema Eurodac oziroma sistema ECRIS-TCN, kolikor hrani biometrične predloge in omogoča iskanje z biometričnimi podatki;
  - (b) varna komunikacijska infrastruktura med skupno BMS, centralnim SIS in CIR.
3. Skupno BMS razvija in tehnično upravlja eu-LISA.

### Člen 13

#### **Hramba biometričnih predlog v skupni storitvi za ugotavljanje ujemanja biometričnih podatkov**

1. Skupna BMS hrani biometrične predloge, ki jih pridobi iz naslednjih biometričnih podatkov:
  - (a) podatkov iz člena 20(3)(w) in (y), razen podatkov o odtisih dlani, Uredbe (EU) 2018/1862;
  - (b) podatkov iz člena 5(1)(b) in (2) Uredbe (EU) 2019/816.

Biometrične predloge se v skupni BMS hranijo smiselno ločeno glede na informacijski sistem EU, iz katerega podatki izvirajo.

2. Za vsak niz podatkov iz odstavka 1 skupna BMS v vsako biometrično predlogo vključi sklic na informacijske sisteme EU, v katerih se hranijo zadevni biometrični podatki, in sklic na dejanske evidence v teh informacijskih sistemih EU.
3. Biometrične predloge se vnesejo v skupno BMS šele po samodejnem pregledu kakovosti biometričnih podatkov, ki so bili dodani enemu od informacijskih sistemov EU, s katerim skupna BMS preveri, ali so izpolnjeni minimalni standardi kakovosti podatkov.
4. Pri hrambi podatkov iz odstavka 1 morajo biti izpolnjeni standardi kakovosti iz člena 37(2).
5. Komisija z izvedbenim aktom določi zahteve glede učinkovitosti delovanja in praktične ureditve za spremljanje učinkovitosti delovanja skupne BMS, s čimer zagotovi, da je učinkovitost biometričnih iskanj primerna za postopke, pri katerih je čas bistvenega pomena, kot so mejni pregledi in identifikacije. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 70(2).

### Člen 14

#### **Iskanje biometričnih podatkov prek skupne storitve za ugotavljanje ujemanja biometričnih podatkov**

Za iskanje biometričnih podatkov, ki se hranijo v CIR in SIS, CIR in SIS uporabljata biometrične predloge, ki se hranijo v skupni BMS. Poizvedbe na podlagi biometričnih podatkov se opravljajo v skladu z nameni iz te uredbe ter uredb (ES) št. 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 in (EU) 2019/816.

### Člen 15

#### **Hramba podatkov v skupni storitvi za ugotavljanje ujemanja biometričnih podatkov**

Podatki iz člena 13(1) in (2) se hranijo v skupni BMS le, dokler se zadevni biometrični podatki hranijo v CIR ali SIS. Podatki se samodejno izbrišejo iz skupne BMS.

## Člen 16

**Vodenje dnevnikov**

1. Brez poseganja v člena 12 in 18 Uredbe (EU) 2018/1862 ter člen 29 Uredbe (EU) 2019/816 eu-LISA vodi dnevnik o vseh postopkih obdelave podatkov v skupni BMS. Ti dnevniki vključujejo naslednje:

- (a) državo članico ali agencijo Unije, ki sproži poizvedbo;
- (b) zgodovino nastanka in hrambe biometričnih predlog;
- (c) informacijske sisteme EU, v katerih se je poizvedovalo na podlagi biometričnih predlog, ki se hranijo v skupni BMS;
- (d) datum in čas poizvedbe;
- (e) vrsto biometričnih podatkov, uporabljenih za sprožitev poizvedbe;
- (f) rezultate poizvedbe ter datum in čas rezultata.

2. Vsaka država članica vodi dnevnik o poizvedbah, ki jih opravijo njeni organi in osebje teh organov, ki je pooblaščen za uporabo skupne BMS. Vsaka agencija Unije vodi dnevnik o poizvedbah, ki jih opravi njeno pooblaščen osebje.

3. Dnevniki iz odstavkov 1 in 2 se lahko uporabljajo izključno za spremljanje varstva podatkov, vključno s preverjanjem dopustnosti poizvedbe in zakonitosti obdelave podatkov, in za zagotavljanje varnosti in celovitosti podatkov. Ti dnevniki se z ustreznimi ukrepi zaščitijo pred nepooblaščenim dostopom in izbrišejo po enem letu od njihovega nastanka. Če so dnevniki potrebni za že začete postopke spremljanja, se izbrišejo, ko niso več potrebni za postopke spremljanja.

**POGLAVJE IV****Skupno odložišče podatkov o identiteti**

## Člen 17

**Skupno odložišče podatkov o identiteti**

1. Skupno odložišče podatkov o identiteti (CIR), ki ustvari individualno dokumentacijo za vsako osebo, ki je evidentirana v SVI, VIS, ETIAS, sistemu Eurodac ali sistemu ECRIS-TCN, in vsebuje podatke iz člena 18, se vzpostavi z namenom, da se olajša in pomaga pri pravilni identifikaciji oseb, registriranih v SVI, VIS, ETIAS, sistemu Eurodac in sistemu ECRIS-TCN v skladu s členom 20, podpre delovanje MID v skladu s členom 21 ter olajša in racionalizira dostop imenovanih organov in Europolu do EES, VIS, ETIAS in sistema Eurodac, kadar je to potrebno za preprečevanje, odkrivanje ali preiskovanje terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj v skladu s členom 22.

2. CIR sestavljajo:

- (a) centralna infrastruktura, ki nadomesti centralne sisteme SVI, VIS, ETIAS, sistema Eurodac in sistema ECRIS-TCN, kolikor hrani podatke iz člena 18;
- (b) varen komunikacijski kanal med CIR, državami članicami in agencijami Unije, ki so upravičene do uporabe CIR v skladu s pravom Unije in nacionalnim pravom;
- (c) varna komunikacijska infrastruktura med CIR, SVI, VIS, ETIAS, sistemom Eurodac, sistemom ECRIS-TCN ter centralno infrastrukturo ESP, skupne BMS in MID.

3. CIR razvija in tehnično upravlja eu-LISA.

4. Kadar je zaradi izpada delovanja CIR tehnično nemogoče poizvedovati v CIR za namene identifikacije osebe v skladu s členom 20, za odkrivanje več identitet v skladu s členom 21 ali za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj v skladu s členom 22, eu-LISA o tem samodejno obvesti uporabnike CIR.

5. eu-LISA za CIR v sodelovanju z državami članicami uvede kontrolni dokument vmesnika, ki temelji na UMF iz člena 38.

## Člen 18

**Podatki v skupnem odložišču podatkov o identiteti**

1. CIR hrani naslednje podatke, ki so logično ločeni glede na informacijski sistem, iz katerega izvirajo: podatke iz člena 5(1)(b) in (2) ter naslednje podatke, navedene v členu 5(1)(a) Uredbe (EU) 2019/816: priimek, ime ali imena, datum rojstva, kraj rojstva (mesto in država), državljanstvo ali državljanstva, spol in po potrebi prejšnje ime ali imena, psevdonime ali vzdevke ter informacije o potnih listinah, kadar so na voljo.
2. Za vsak niz podatkov iz odstavka 1 CIR vključi sklic na informacijske sisteme EU, katerim podatki pripadajo.
3. Organi, ki dostopajo do CIR, to storijo v skladu s svojimi pravicami dostopa na podlagi pravnih instrumentov, ki urejajo informacijske sisteme EU, in v nacionalnega prava, ter v skladu s svojimi pravicami dostopa v skladu s to uredbo za namene iz členov 20, 21 in 22.
4. Za vsak niz podatkov iz odstavka 1 CIR vključi sklic na dejansko evidenco v informacijskih sistemih EU, kateri podatki pripadajo.
5. Pri hrambi podatkov iz odstavka 1 morajo biti izpolnjeni standardi kakovosti iz člena 37(2).

## Člen 19

**Dodajanje, spreminjanje in brisanje podatkov v skupnem odložišču podatkov o identiteti**

1. Kadar se podatki v sistemu Eurodac ali sistemu ECRIS-TCN dodajo, spremenijo ali izbrišejo, se podatki iz člena 18, ki se hranijo v individualni dokumentaciji v CIR, ustrezno samodejno dodajo, spremenijo ali izbrišejo.
2. Kadar se v MID v skladu s členom 32 ali 33 vzpostavi bela ali rdeča povezava med podatki iz dveh ali več informacijskih sistemov EU, ki jih zajema CIR, namesto da ustvari novo individualno dokumentacijo, CIR doda nove podatke individualni dokumentaciji, ki vsebuje povezane podatke.

## Člen 20

**Dostop do skupnega odložišča podatkov o identiteti za namene identifikacije**

1. Poizvedbe v CIR opravi policijski organ v skladu z odstavkoma 2 in 5 le v naslednjih okoliščinah:
  - (a) kadar policijski organ ne more identificirati osebe, ker nima potne listine ali drugega verodostojnega dokumenta, ki navaja identiteto te osebe;
  - (b) kadar obstajajo dvomi glede podatkov o identiteti, ki jih je navedla oseba;
  - (c) kadar obstaja dvom o verodostojnosti potne listine ali drugega verodostojnega dokumenta, ki ga je oseba predložila;
  - (d) kadar obstaja dvom glede identitete imetnika potne listine ali drugega verodostojnega dokumenta, ali
  - (e) kadar oseba ne more ali noče sodelovati.

Take poizvedbe niso dovoljene za mladoletnike, mlajše od 12 let, razen če je to v največjo korist otroka.

2. Kadar gre za katero od okoliščin iz odstavka 1 in je policijski organ za to pooblaščen z nacionalnimi zakonodajnimi ukrepi iz odstavka 5, lahko izključno za namene identifikacije osebe poizveduje v CIR na podlagi biometričnih podatkov te osebe, pridobljenih na kraju samem med ugotavljanjem identitete, pod pogojem, da je bil postopek pričet v prisotnosti te osebe.

3. Kadar poizvedba pokaže, da se podatki o tej osebi hranijo v CIR, ima policijski organ dostop za vpogled v podatke iz člena 18(1).

Kadar biometričnih podatkov osebe ni mogoče uporabiti ali kadar je poizvedba na podlagi teh podatkov neuspešna, se poizvedba opravi na podlagi podatkov o identiteti osebe in podatkov o potni listini ali podatkov o identiteti, ki jih navede ta oseba.

4. Kadar je policijski organ z nacionalnimi zakonodajnimi ukrepi iz odstavka 6 za to pooblaščen, lahko v primeru naravne nesreče, nezgode ali terorističnega napada in izključno za namen identifikacije neznanih oseb, ki se ne morejo same identificirati, ali neidentificiranih človeških ostankov poizveduje v CIR na podlagi biometričnih podatkov teh oseb.
5. Države članice, ki želijo uporabiti možnost iz odstavka 2, sprejmejo nacionalne zakonodajne ukrepe. Pri tem upoštevajo potrebo po preprečevanju vsakršne diskriminacije državljanov tretjih držav. V takih zakonodajnih ukrepih se določijo natančni nameni identifikacije v okviru namenov iz člena 2(1)(b) in (c). Določijo tudi pristojne policijske organe ter postopke, pogoje in merila za ugotavljanje identitete.
6. Države članice, ki želijo izkoristiti možnost iz odstavka 4, sprejmejo nacionalne zakonodajne ukrepe za določitev zadevnih postopkov, pogojev in meril.

#### Člen 21

##### **Dostop do skupnega odložišča podatkov o identiteti za namene odkrivanja več identitet**

1. Kadar poizvedba v CIR privede do rumene povezave v skladu s členom 28(4), ima organ iz člena 29, ki je pristojen za ročno preverjanje različnih identitet, izključno za namene preverjanja dostop do podatkov iz člena 18(1) in (2), ki se hranijo v CIR, povezane z rumeno povezavo.
2. Kadar poizvedba v CIR privede do rdeče povezave v skladu s členom 32, imajo organi iz člena 26(2) izključno za namene boja proti identitetnim prevaram dostop do podatkov iz člena 18(1) in (2), ki se hranijo v CIR, povezane z rdečo povezavo.

#### Člen 22

##### **Poizvedovanje v skupnem odložišču podatkov o identiteti za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj**

1. V posebnih primerih, kadar obstajajo utemeljeni razlogi za domnevo, da bo iskanje po informacijskih sistemih EU prispevalo k preprečevanju, odkrivanju ali preiskovanju terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj, zlasti kadar obstaja sum, da je osumljenec, storilec ali žrtev terorističnega kaznivega dejanja ali drugega hudega kaznivega dejanja oseba, katere podatki se hranijo v sistemu Eurodac, lahko imenovani organi in Europol uporabijo CIR za pridobitev informacij o obstoju podatkov o določeni osebi v sistemu Eurodac.
2. Kadar v odgovor na poizvedbo CIR pokaže, da so podatki o zadevni osebi v sistemu Eurodac, CIR imenovanim organom in Europolu pošlje odgovor v obliki sklica iz člena 18(2), da sistem Eurodac vsebuje ujemajoče se podatke. Odgovor CIR mora biti takšen, da ne ogroža varnosti podatkov.

Odgovor, ki pokaže, da so podatki o tej osebi v sistemu Eurodac, se uporabi le za predložitev zahteve za popoln dostop ob upoštevanju pogojev in postopkov, določenih v pravnem instrumentu, ki ureja tak dostop.

V primeru ujemanja ali več ujemanj imenovani organ ali Europol zahteva popoln dostop do vsaj enega od informacijskih sistemov, v katerem je prišlo do ujemanja.

Kadar se takšen popolni dostop izjemoma ne zahteva, imenovani organi zabeležijo obrazložitev, zakaj niso podali take zahteve, ki jo je mogoče povezati z nacionalno dokumentacijo. Europol obrazložitev vpiše v ustrezno dokumentacijo.

3. Za popoln dostop do podatkov v sistemu Eurodac za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj še naprej veljajo pogoji in postopki iz pravnega instrumenta, ki ureja tak dostop.

## Člen 23

**Hramba podatkov v skupnem odložišču podatkov o identiteti**

1. Podatki iz člena 18(1), (2) in (4) se samodejno izbrišejo iz CIR v skladu z določbami o hrambi podatkov iz Uredbe (EU) 2019/816.
2. Individualna dokumentacija se hrani v CIR le, dokler se ustrezni podatki, ki jih vsebuje CIR, hranijo vsaj v enem od informacijskih sistemov EU. Vzpostavitev povezave ne vpliva na obdobje hrambe posameznih povezanih podatkov.

## Člen 24

**Vodenje dnevnikov**

1. Brez poseganja v člen 29 Uredbe (EU) 2019/816 eu-LISA vodi dnevnik o vseh postopkih obdelave podatkov v CIR v skladu z odstavki 2, 3 in 4 tega člena.
2. eu-LISA vodi dnevnik o vseh postopkih obdelave podatkov v skladu s členom 20 v CIR. Ti dnevniki vključujejo naslednje:
  - (a) državo članico ali agencijo Unije, ki sproži poizvedbo;
  - (b) namen dostopa uporabnika, ki poizveduje prek CIR;
  - (c) datum in čas poizvedbe;
  - (d) vrsto podatkov, uporabljenih za sprožitev poizvedbe;
  - (e) rezultate poizvedbe.
3. eu-LISA vodi dnevnik o vseh postopkih obdelave podatkov v skladu s členom 21 v CIR. Ti dnevniki vključujejo naslednje:
  - (a) državo članico ali agencijo Unije, ki sproži poizvedbo;
  - (b) namen dostopa uporabnika, ki poizveduje prek CIR;
  - (c) datum in čas poizvedbe;
  - (d) kadar se vzpostavi povezava – podatke, uporabljene za sprožitev poizvedbe in rezultate poizvedbe z navedbo informacijskega sistema EU, iz katerega so bili podatki prejeti.
4. eu-LISA vodi dnevnik o vseh postopkih obdelave podatkov v skladu s členom 22 v CIR. Ti dnevniki vključujejo naslednje:
  - (a) datum in čas poizvedbe;
  - (b) podatke, uporabljene za sprožitev poizvedbe;
  - (c) rezultate poizvedbe;
  - (d) državo članico ali agencijo Unije, ki poizveduje v CIR.

Dnevnik takega dostopa redno preverja pristojni nadzorni organ v skladu s členom 41 Direktive (EU) 2016/680 ali Evropski nadzornik za varstvo podatkov v skladu s členom 43 Uredbe (EU) 2016/794, in sicer v časovnih presledkih, ki niso daljši od šest mesecev, da preveri, ali so izpolnjeni postopki in pogoji iz člena 22(1) in (2) te uredbe.

5. Vsaka država članica vodi dnevnik o poizvedbah, ki jih opravijo njeni organi in osebje teh organov, ki je pooblašeno za uporabo CIR v skladu s členi 20, 21 in 22. Vsaka agencija Unije vodi dnevnik o poizvedbah, ki jih opravi njeno ustrezno pooblašeno osebje v skladu s členoma 21 in 22.

Poleg tega vsaka država članica za vsak dostop do CIR v skladu s členom 22 vodi naslednje dnevnik:

- (a) sklic na nacionalno dokumentacijo;
- (b) namen dostopa;
- (c) edinstveno uporabniško identiteto uradnika, ki je opravil poizvedbo, in uradnika, ki je dal nalog za poizvedbo, v skladu z nacionalnimi pravili.

6. Europol v skladu z Uredbo (EU) 2016/794 za vsak dostop do CIR v skladu s členom 22 te uredbe vodi dnevnik o edinstveni uporabniški identiteti uradnika, ki je opravil poizvedbo, in uradniku, ki je dal nalog za poizvedbo.

7. Dnevnik iz odstavkov 2 do 6 se lahko uporabljajo izključno za spremljanje varstva podatkov, vključno s preverjanjem dopustnosti poizvedbe in zakonitosti obdelave podatkov, in za zagotavljanje varnosti in celovitosti podatkov. Ti dnevnik se z ustreznimi ukrepi zaščitijo pred nepooblaščenim dostopom in izbrišejo po enem letu od njihovega nastanka. Če so dnevnik potrebni za že začete postopke spremljanja, se izbrišejo, ko niso več potrebni za postopke spremljanja.

8. eu-LISA v individualni dokumentaciji hrani dnevnik v zvezi z zgodovino podatkov. eu-LISA take dnevnik samodejno izbriše, ko se izbrišejo podatki.

## **POGLAVJE V**

### **Detektor več identitet**

#### *Člen 25*

### **Detektor več identitet**

1. Za namene podpiranja delovanja CIR ter ciljev SVI, VIS, ETIAS, sistema Eurodac, SIS in sistema ECRIS-TCN se vzpostavi detektor več identitet (MID), ki vzpostavlja in hrani dokumentacijo o potrditvi identitete iz člena 34, ki vsebuje povezave med podatki v informacijskih sistemih EU, ki jih zajema CIR, in SIS ter omogoča odkrivanje več identitet z namenom lažjega ugotavljanja identitete in boja proti identitetnim prevaram.

2. MID sestavljajo:

- (a) centralna infrastruktura, ki hrani povezave in sklice na informacijske sisteme EU;
- (b) varna komunikacijska infrastruktura za povezavo MID s SIS ter centralnima infrastrukturama ESP in CIR.

3. MID razvija in tehnično upravlja eu-LISA.

#### *Člen 26*

### **Dostop do detektorja več identitet**

1. Za namene ročnega preverjanja različnih identitet iz člena 29 se dostop do podatkov iz člena 34, ki se hranijo v MID, odobri:

- (a) uradu SIRENE države članice, ki izda ali posodobi razpis ukrepa v skladu z Uredbo (EU) 2018/1862;
- (b) centralnim organom države članice izreka obsodbe pri zapisovanju ali spreminjanju podatkov v sistemu ECRIS-TCN v skladu s členom 5 ali 9 Uredbe (EU) 2019/816.

2. Organi držav članic in agencije Unije, ki imajo dostop do vsaj enega informacijskega sistema EU, ki ga zajema CIR, ali do SIS, imajo dostop do podatkov iz člena 34(a) in (b) v zvezi z rdečimi povezavami iz člena 32.

3. Organi držav članic in agencije Unije imajo dostop do belih povezav iz člena 33, če imajo dostop do obeh informacijskih sistemov EU, ki vsebujeta podatke med katerimi je bila vzpostavljena bela povezava.

4. Organi držav članic in agencije Unije imajo dostop do zelenih povezav iz člena 31, če imajo dostop do obeh informacijskih sistemov EU, ki vsebujejo podatke med katerimi je bila vzpostavljena zelena povezava, poizvedba v teh informacijskih sistemih pa je razkrila ujemanja z obema nizoma povezanih podatkov.

## Člen 27

**Odkrivanje več identitet**

1. Odkrivanje več identitet v CIR in SIS se sproži pri:
  - (a) izdaji ali posodobitvi razpisa ukrepa za osebo v SIS v skladu s poglavji VI do IX Uredbe (EU) 2018/1862;
  - (b) pripravi ali spremembi podatkovnega zapisa v sistemu ECRIS-TCN v skladu s členom 5 ali 9 Uredbe (EU) 2019/816.
2. Kadar podatki v informacijskem sistemu EU iz odstavka 1 vsebujejo biometrične podatke, CIR in centralni SIS opravita odkrivanje več identitet prek skupne BMS. Skupna BMS primerja biometrične predloge, pridobljene iz novih biometričnih podatkov, z biometričnimi predlogami, ki jih že vsebuje, da preveri, ali se podatki, ki se nanašajo na isto osebo, že hranijo v CIR ali centralnem SIS.
3. Poleg postopka iz odstavka 2 CIR in centralni SIS prek ESP iščeta podatke, ki se hranijo v centralnem SIS oziroma CIR, z uporabo naslednjih podatkov:
  - (a) priimkov, imen, imen in priimkov ob rojstvu, prej uporabljenih imen in priimkov ter privzetih imen, kraja rojstva, datuma rojstva, spola in državljanstev, kakor so navedeni v členu 20(3) Uredbe (EU) 2018/1862;
  - (b) priimka, imena ali imen, datuma rojstva, kraja rojstva (mesto in država), državljanstva ali državljanstev in spola, kakor so navedeni v členu 5(1)(a) Uredbe (EU) 2019/816.
4. Poleg postopka iz odstavkov 2 in 3 CIR in centralni SIS prek ESP iščeta podatke, ki se hranijo v centralnem SIS in CIR z uporabo podatkov o potni listini.
5. Odkrivanje več identitet se sproži le za primerjavo podatkov iz enega informacijskega sistema EU s podatki iz drugih informacijskih sistemov EU.

## Člen 28

**Rezultati odkrivanja več identitet**

1. Kadar poizvedbe iz člena 27(2), (3) in (4) ne privedejo do ujemanja, se postopki iz člena 27(1) nadaljujejo v skladu s pravnimi instrumenti, ki jih urejajo.
2. Kadar poizvedba iz člena 27(2), (3) in (4) privede do enega ali več ujemanj, CIR in, kadar je to primerno, SIS vzpostavi povezavo med podatki, uporabljenimi za sprožitev poizvedbe, in podatki, ki so privedli do ujemanja.

V primeru več ujemanj se povezava vzpostavi med vsemi podatki, ki so privedli do ujemanja. Kadar so bili podatki že povezani, se obstoječa povezava razširi na podatke, uporabljene za sprožitev poizvedbe.
3. Kadar poizvedba iz člena 27(2), (3) in (4) privede do enega ali več ujemanj in so podatki o identiteti iz povezanih dokumentacij enaki ali podobni, se vzpostavi bela povezava v skladu s členom 33.
4. Kadar poizvedba iz člena 27(2), (3) in (4) privede do enega ali več ujemanj in podatkov o identiteti iz povezanih dokumentacij ni mogoče šteti za podobne, se vzpostavi rumena povezava v skladu s členom 30 in uporabi se postopek iz člena 29.
5. Komisija sprejme delegirane akte v skladu s členom 69, s katerimi določi postopke za opredelitev primerov, v katerih se lahko podatki o identiteti štejejo za enake ali podobne.
6. Povezave se hranijo v dokumentaciji o potrditvi identitete iz člena 34.
7. Komisija v sodelovanju z eu-LISA z izvedbenimi akti določi tehnična pravila o vzpostavljanju povezav med podatki iz različnih informacijskih sistemov EU. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 70(2).

## Člen 29

**Ročno preverjanje različnih identitet in pristojni organi**

1. Brez poseganja v odstavek 2 organ, ki je pristojen za ročno preverjanje različnih identitet, pomeni:
  - (a) urad SIRENE države članice za ujemanja, do katerih je prišlo pri izdaji ali posodobitvi razpisa ukrepa v SIS v skladu z Uredbo (EU) 2018/1862;
  - (b) centralne organe države članice izreka obsodbe za ujemanja pri zapisovanju ali spreminjanju podatkov v sistemu ECRIS-TCN v skladu s členom 5 ali 9 Uredbe (EU) 2019/816.

MID navede organ, ki je pristojen za ročno preverjanje različnih identitet v dokumentaciji o potrditvi identitete.

2. Organ, ki je pristojen za ročno preverjanje različnih identitet v dokumentaciji o potrditvi identitete, je urad SIRENE države članice, ki je izdala razpis ukrepa, kadar se vzpostavi povezava do podatkov v razpisu ukrepa:

- (a) za osebe, za katere se zahteva prijetje zaradi predaje ali izročitve iz člena 26 Uredbe (EU) 2018/1862;
- (b) za pogrešane ali ranljive osebe iz člena 32 Uredbe (EU) 2018/1862;
- (c) za osebe, iskane zaradi sodelovanja v sodnem postopku iz člena 34 Uredbe (EU) 2018/1862;
- (d) za osebe zaradi prikrite kontrole, poizvedovalne kontrole ali namenske kontrole iz člena 36 Uredbe (EU) 2018/1862.

3. Organ, ki je pristojen za ročno preverjanje različnih identitet, ima dostop do povezanih podatkov v zadevni dokumentaciji o potrditvi identitete in povezanih podatkov o identiteti v CIR in, kadar je to primerno, v SIS. Organ brez odlašanja oceni različne identitete. Ko je ta ocena zaključena, organ posodobi povezavo v skladu s členi 31, 32 in 33 ter jo brez odlašanja doda dokumentaciji o potrditvi identitete.

4. Kadar je vzpostavljenih več povezav, organ, ki je pristojen za ročno preverjanje različnih identitet, oceni vsako povezavo posebej.

5. Kadar so podatki, ki so privedli do ujemanja, že bili povezani, organ, ki je pristojen za ročno preverjanje različnih identitet, upošteva obstoječe povezave pri oceni novih povezav.

## Člen 30

**Rumena povezava**

1. Kadar ročno preverjene različnih identitet še ni bilo opravljeno, se povezava med podatki iz dveh ali več informacijskih sistemov EU razvrsti kot rumena v katerem koli od naslednjih primerov:

- (a) povezani podatki vključujejo enake biometrične podatke, vendar podobne ali različne podatke o identiteti;
- (b) povezani podatki vključujejo različne podatke o identiteti, vendar enake podatke o potni listini, in vsaj eden od informacijskih sistemov EU ne vsebuje biometričnih podatkov o zadevni osebi;
- (c) povezani podatki vključujejo enake podatke o identiteti, vendar različne biometrične podatke;
- (d) povezani podatki vključujejo podobne ali različne podatke o identiteti in enake podatke o potni listini, vendar različne biometrične podatke.

2. Kadar se povezava razvrsti kot rumena v skladu z odstavkom 1, se uporabi postopek iz člena 29.

## Člen 31

**Zelena povezava**

1. Povezava med podatki iz dveh ali več informacijskih sistemov EU se razvrsti kot zelena, kadar:
  - (a) povezani podatki vključujejo različne biometrične podatke, vendar enake podatke o identiteti, organ, pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se povezani podatki nanašajo na različni osebi;
  - (b) povezani podatki vključujejo različne biometrične podatke, vendar podobne ali različne podatke o identiteti ter enake podatke o potni listini, organ, pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se povezani podatki nanašajo na različni osebi;
  - (c) povezani podatki vključujejo različne podatke o identiteti, vendar enake podatke o potni listini, in vsaj eden od informacijskih sistemov EU ne vsebuje biometričnih podatkov o osebi, organ, pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se povezani podatki nanašajo na dve različni osebi.
2. Kadar se poizveduje v CIR ali SIS in kadar med podatki v dveh ali več informacijskih sistemih EU obstaja zelena povezava, MID navede, da se podatki o identiteti v povezanih podatkih ne nanašajo na isto osebo.
3. Če ima organ države članice dokaze, ki kažejo, da je bila zelena povezava nepravilno zabeležena v MID, ni posodobljena ali da je bila obdelava podatkov v MID ali informacijskih sistemih EU v nasprotju s to uredbo, preveri zadevne podatke, ki se hranijo v CIR in SIS, ter po potrebi brez odlašanja popravi ali izbriše povezavo v MID. Ta organ države članice brez odlašanja obvesti državo članico, pristojno za ročno preverjanje različnih identitet.

## Člen 32

**Rdeča povezava**

1. Povezava med podatki iz dveh ali več informacijskih sistemov EU se razvrsti kot rdeča v katerem koli od naslednjih primerov:
  - (a) povezani podatki vključujejo enake biometrične podatke, vendar podobne ali različne podatke o identiteti, organ, pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se neupravičeno nanašajo na isto osebo;
  - (b) povezani podatki vključujejo enake, podobne ali različne podatke o identiteti in enake podatke o potovalni listini, vendar različne biometrične podatke, organ, pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se povezani podatki nanašajo na dve različni osebi, od katerih vsaj ena neupravičeno uporablja isto potno listino;
  - (c) povezani podatki vključujejo enake podatke o identiteti, vendar različne biometrične podatke in različne ali nobenih podatkov o potni listini, organ, pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se povezani podatki neupravičeno nanašajo na dve različni osebi;
  - (d) povezani podatki vključujejo različne podatke o identiteti, vendar enake podatke o potni listini, pri čemer vsaj eden od informacijskih sistemov EU ne vsebuje biometričnih podatkov o zadevni osebi, organ, pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se povezani podatki neupravičeno nanašajo na isto osebo.
2. Kadar se poizveduje v CIR ali SIS in kadar med dvema ali več informacijskimi sistemi EU obstaja rdeča povezava, MID navede podatke iz člena 34. Po rdeči povezavi se nadalje ukrepa v skladu s pravom Unije in nacionalnim pravom, vse pravne posledice za zadevno osebo pa morajo temeljiti le na ustreznih podatkih o tej osebi. Zadevna oseba zgolj zaradi obstoja rdeče povezave ne sme utrpeti pravnih posledic.
3. Kadar se vzpostavi rdeča povezava med podatki iz SVI, VIS, ETIAS, sistema Eurodac ali sistema ECRIS-TCN, se individualna dokumentacija, ki se hrani v CIR, posodobi v skladu s členom 19(2).

4. Brez poseganja v določbe v zvezi z obdelavo razpisov ukrepov v SIS, vsebovane v uredbah (EU) 2018/1860, (EU) 2018/1861 in (EU) 2018/1862, ter brez poseganja v omejitve, potrebne za zaščito varnosti in javnega reda, preprečevanje kaznivih dejanj in zagotavljanje, da ne bo ogrožena nobena nacionalna preiskava, organ, pristojen za ročno preverjanje različnih identitet, v primeru rdeče povezave zadevno osebo obvesti o obstoju več nezakonitih podatkov o identiteti ter ji zagotovi enotno identifikacijsko številko iz člena 34(c) te uredbe, sklic na organ, pristojen za ročno preverjanje različnih identitet, iz člena 34(d) te uredbe, in spletni naslov portala, vzpostavljenega v skladu s členom 49 te uredbe.

5. Informacije iz odstavka 4 v pisni obliki na standardnem obrazcu zagotovi organ, pristojen za ročno preverjanje različnih identitet. Komisija z izvedbenimi akti določi vsebino in obliko tega obrazca. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 70(2).

6. Kadar se vzpostavi rdeča povezava, MID samodejno obvesti organe, pristojne za povezane podatke.

7. Če ima organ države članice ali agencija Unije, ki ima dostop do CIR ali SIS, dokaze, ki kažejo, da je bila rdeča povezava nepravilno zabeležena v MID, ali da so bili podatki, obdelani v MID, CIR ali SIS, obdelani v nasprotju s to uredbo, ta organ ali agencija preveri zadevne podatke, hranjene v CIR in SIS, ter:

(a) kadar povezava zadeva enega od razpisov ukrepov v SIS iz člena 29(2), o tem takoj obvesti ustrezni urad SIRENE države članice, ki je izdala razpis ukrepa v SIS;

(b) v vseh drugih primerih takoj popravi ali izbriše povezavo iz MID.

Če se z uradom SIRENE stopi v stik v skladu s točko (a) prvega pododstavka, preveri dokaze, ki jih je predložil organ države članice ali agencija Unije, in po potrebi takoj popravi ali izbriše povezavo v MID.

Organ države članice, ki pridobi dokaze, državo članico, pristojno za ročno preverjanje različnih identitet, brez odlašanja obvesti o vsakem ustreznem popravku ali izbrisu rdeče povezave.

### Člen 33

#### Bela povezava

1. Povezava med podatki iz dveh ali več informacijskih sistemov EU se razvrsti kot bela v katerem koli od naslednjih primerov:

(a) povezani podatki vključujejo enake biometrične podatke in enake ali podobne podatke o identiteti;

(b) povezani podatki vključujejo enake ali podobne podatke o identiteti, enake podatke o potni listini, vsaj eden od informacijskih sistemov EU pa ne vsebuje biometričnih podatkov o zadevni osebi;

(c) povezani podatki vključujejo enake biometrične podatke, enake podatke o potni listini, vendar podobne podatke o identiteti;

(d) povezani podatki vključujejo enake biometrične podatke, vendar podobne ali različne podatke o identiteti, organ, ki je pristojen za ročno preverjanje različnih identitet, pa je sklenil, da se povezani podatki upravičeno nanašajo na isto osebo.

2. Kadar se poizveduje v CIR ali SIS in kadar med dvema ali več informacijskimi sistemi EU obstaja bela povezava, MID navede, da se podatki o identiteti v povezanih podatkih nanašajo na isto osebo. V odgovoru poizvedovanih informacijskih sistemov EU se, kadar je to primerno, navedejo vsi povezani podatki osebe, kar privede do ujemanja na podlagi podatkov, ki so povezani z belo povezavo, če ima organ, ki je sprožil poizvedbo, dostop do povezanih podatkov na podlagi prava Unije ali nacionalnega prava.

3. Kadar se vzpostavi bela povezava med podatki iz SVI, VIS, ETIAS, sistema Eurodac ali sistema ECRIS-TCN, se individualna dokumentacija, ki se hrani v CIR, posodobi v skladu s členom 19(2).

4. Brez poseganja v določbe v zvezi z obdelavo razpisov ukrepov v SIS, vsebovane v uredbah (EU) 2018/1860, (EU) 2018/1861 in (EU) 2018/1862, ter brez poseganja v omejitve, potrebne za zaščito varnosti in javnega reda, preprečevanje kaznivih dejanj in zagotavljanje varnosti nacionalnih preiskav, organ, pristojen za ročno preverjanje različnih identitet, v primeru bele povezave po ročnem preverjanju različnih identitet zadevno osebo obvesti o obstoju podobnih ali različnih podatkov o identiteti ter ji zagotovi enotno identifikacijsko številko iz člena 34(c) te uredbe, sklic na organ, pristojen za ročno preverjanje različnih identitet, iz člena 34(d) te uredbe, in spletni naslov portala, vzpostavljenega v skladu s členom 49 te uredbe.

5. Če ima organ države članice dokaze, ki kažejo, da je bila bela povezava nepravilno evidentirana v MID, ni posodobljena ali da je bila obdelava podatkov v MID ali informacijskih sistemih EU v nasprotju s to uredbo, preveri zadevne podatke, ki se hranijo v CIR in SIS, ter po potrebi brez odlašanja popravi ali izbriše povezavo v MID. Ta organ države članice brez odlašanja obvesti državo članico, pristojno za ročno preverjanje različnih identitet.

6. Informacije iz odstavka 4 v pisni obliki na standardnem obrazcu zagotovi organ, pristojen za ročno preverjanje različnih identitet. Komisija z izvedbenimi akti določi vsebino in obliko tega obrazca. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 70(2).

#### Člen 34

##### **Dokumentacija o potrditvi identitete**

Dokumentacija o potrditvi identitete vsebuje naslednje podatke:

- (a) povezave iz členov od 30 do 33;
- (b) sklic na informacijske sisteme EU, ki vsebujejo povezane podatke;
- (c) enotno identifikacijsko številko, ki omogoča pridobivanje povezanih podatkov iz zadevnih informacijskih sistemov EU;
- (d) organ, pristojen za ročno preverjanje različnih identitet;
- (e) datum vzpostavitve povezave ali morebitne njene posodobitve.

#### Člen 35

##### **Hramba podatkov v detektorju več identitet**

Dokumentacije o potrditvi identitete in podatki v njih, vključno s povezavami, se hranijo v MID le, dokler se povezani podatki hranijo v dveh ali več informacijskih sistemih EU. Podatki se samodejno izbrišejo iz MID.

#### Člen 36

##### **Vodenje dnevnikov**

- 1. eu-LISA vodi dnevnik o vseh postopkih obdelave podatkov v MID. Ti dnevniki vključujejo naslednje:
  - (a) državo članico, ki sproži poizvedbo;
  - (b) namen dostopa uporabnika;
  - (c) datum in čas poizvedbe;
  - (d) vrsto podatkov, uporabljenih za sprožitev poizvedbe;
  - (e) sklic na povezane podatke;
  - (f) zgodovino dokumentacije o potrditvi identitete.

2. Vsaka država članica vodi dnevnike o poizvedbah, ki jih opravijo njeni organi in osebje teh organov, ki je pooblaščen za uporabo MID. Vsaka agencija Unije vodi dnevnike o poizvedbah, ki jih opravi njeno pooblaščen osebje.

3. Dnevnik iz odstavkov 1 in 2 se lahko uporabljajo izključno za spremljanje varstva podatkov, vključno s preverjanjem dopustnosti poizvedbe in zakonitosti obdelave podatkov, in za zagotavljanje varnosti in celovitosti podatkov. Ti dnevniki se z ustreznimi ukrepi zaščitijo pred nepooblaščenim dostopom in izbrišejo po enem letu od njihovega nastanka. Če so dnevniki potrebni za že začete postopke spremljanja, se izbrišejo, ko niso več potrebni za postopke spremljanja.

## POGLAVJE VI

### Ukrepi za podporo interoperabilnosti

#### Člen 37

#### Kakovost podatkov

1. Brez poseganja v odgovornosti držav članic glede kakovosti podatkov, vnesenih v sisteme, eu-LISA vzpostavi samodejne mehanizme in postopke za nadzor kakovosti podatkov, shranjenih v SIS, sistemu Eurodac, sistemu ECRIS-TCN, skupni BMS in CIR.

2. eu-LISA izvaja mehanizme za ocenjevanje točnosti skupne BMS, skupne kazalnike kakovosti podatkov ter minimalne standarde kakovosti za hrambo podatkov v SIS, sistemu Eurodac, sistemu ECRIS-TCN, skupni BMS in CIR.

V SIS, sistem Eurodac, sistem ECRIS-TCN, skupno BMS, CIR in MID se lahko vnesejo le podatki, ki izpolnjujejo minimalne standarde kakovosti.

3. eu-LISA državam članicam redno poroča o samodejnih mehanizmi in postopkih za nadzor kakovosti podatkov ter o skupnih kazalnikih kakovosti podatkov. eu-LISA tudi redno poroča Komisiji o težavah, ki se pojavijo, in državah članicah, ki jih težave zadevajo. eu-LISA to poročilo na zahtevo predloži tudi Evropskemu parlamentu in Svetu. Poročila iz tega odstavka ne vsebujejo osebnih podatkov.

4. Podrobnosti glede samodejnih mehanizmov in postopkov za nadzor kakovosti podatkov ter glede skupnih kazalnikov kakovosti podatkov in minimalnih standardov kakovosti za hrambo podatkov v SIS, sistemu Eurodac, sistemu ECRIS-TCN, skupni BMS in CIR, zlasti v zvezi z biometričnimi podatki, se določijo v izvedbenih aktih. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 70(2).

5. Komisija eno leto po vzpostavitvi samodejnih mehanizmov in postopkov za nadzor kakovosti podatkov, skupnih kazalnikov kakovosti podatkov ter minimalnih standardov kakovosti podatkov, nato pa vsako leto, oceni, kako države članice izvajajo zahteve glede kakovosti podatkov, in poda morebitna potrebna priporočila. Države članice Komisiji predložijo akcijski načrt za odpravo morebitnih pomanjkljivosti, ugotovljenih v poročilu o oceni, zlasti težav s kakovostjo podatkov, ki izhajajo iz napačnih podatkov v informacijskih sistemih EU. Države članice Komisiji redno poročajo o napredku glede akcijskega načrta do njegove izvedbe v celoti.

Komisija poročilo o oceni posreduje Evropskemu parlamentu, Svetu, Evropskemu nadzorniku za varstvo podatkov, Evropskemu odboru za varstvo podatkov in Agenciji Evropske unije za temeljne pravice, ustanovljeni z Uredbo Sveta (ES) št. 168/2007 <sup>(37)</sup>.

#### Člen 38

#### Univerzalni format sporočil

1. Vzpostavi se standard univerzalnega formata sporočil (UMF). UMF opredeljuje standarde za določene elemente vsebine čezmejne izmenjave informacij med informacijskimi sistemi, organi ali organizacijami na področju pravosodja in notranjih zadev.

<sup>(37)</sup> Uredba Sveta (ES) št. 168/2007 z dne 15. februarja 2007 o ustanovitvi Agencije Evropske unije za temeljne pravice (UL L 53, 22.2.2007, str. 1).

2. Standard UMF se uporablja pri razvoju sistema Eurodac, sistema ECRIS-TCN, ESP, CIR in MID ter, po potrebi, pri razvoju novih modelov za izmenjavo informacij in informacijskih sistemov na področju pravosodja in notranjih zadev s strani eu-LISA ali druge agencije Unije.
3. Komisija sprejme izvedbeni akt za določitev in razvoj standarda UMF iz odstavka 1 tega člena. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 70(2).

#### Člen 39

### Centralni register za poročanje in statistične podatke

1. Vzpostavi se centralni register za poročanje in statistične podatke (CRRS) za namene podpiranja ciljev SIS, sistema Eurodac in sistema ECRIS-TCN v skladu z zadevnimi pravnimi instrumenti, ki urejajo te sisteme, ter za zagotavljanje medsystemske statistične podatke in analitičnega poročanja za namene politike ter operativne namene ter namene kakovosti podatkov.
2. eu-LISA logično ločeno z informacijskim sistemom EU vzpostavi, izvaja in na svojih tehničnih lokacijah gosti CRRS, ki vsebuje podatke, vključno s statističnimi podatki, iz člena 74 Uredbe (EU) 2018/1862 in člena 32 Uredbe (EU) 2019/816. Dostop do CRRS se izključno za namene poročanja in statistične namene dovoli organom iz člena 74 Uredbe (EU) 2018/1862 in člena 32 Uredbe (EU) 2019/816, in sicer z prek nadzorovanega, varnega dostopa in posebnih uporabniških profilov.
3. eu-LISA podatke anonimizira in take anonimizirane podatke evidentira v CRRS. Postopek anonimizacije podatkov je samodejen.

Podatki v CRRS ne smejo omogočati identifikacije posameznikov.

4. CRRS sestavljajo:
  - (a) orodja, potrebna za anonimizacijo podatkov;
  - (b) centralna infrastruktura, ki jo sestavlja register anonimiziranih podatkov;
  - (c) varna komunikacijska infrastruktura za povezavo CRRS s SIS, sistemom Eurodac in sistemom ECRIS-TCN ter s centralnimi infrastrukturami skupne BMS, CIR in MID.
5. Komisija sprejme delegirani akt v skladu s členom 69 za določitev podrobnih pravil o delovanju CRRS, vključno s posebnimi zaščitnimi ukrepi za obdelavo osebnih podatkov na podlagi odstavkov 2 in 3 tega člena, ter pravila o varnosti, ki se uporabljajo za register.

## POGLAVJE VII

### Varstvo podatkov

#### Člen 40

### Upravljavec podatkov

1. V zvezi z obdelavo podatkov v skupni BMS so organi držav članic, ki so upravljavci za sistem Eurodac, SIS oziroma sistem ECRIS-TCN, tudi upravljavci v skladu s točko 7 člena 4 Uredbe (EU) 2016/679 ali točko 8 člena 3 Direktive (EU) 2016/680 v zvezi z biometričnimi predlogami, pridobljenimi iz podatkov iz člena 13 te uredbe, ki jih vnesejo v osnovne sisteme, odgovorni pa so tudi za obdelavo biometričnih predlog v skupni BMS.
2. V zvezi z obdelavo podatkov v CIR so organi držav članic, ki so upravljavci za sistem Eurodac oziroma sistem ECRIS-TCN, tudi upravljavci v skladu s točko 7 člena 4 Uredbe (EU) 2016/679 ali točko 8 člena 3 Direktive (EU) 2016/680 v zvezi s podatki iz člena 18 te uredbe, ki jih vnesejo v osnovne sisteme, odgovorni pa so tudi za obdelavo teh osebnih podatkov v CIR.
3. V zvezi z obdelavo podatkov v MID:
  - (a) je Evropska agencija za mejno in obalno stražo upravljavec podatkov v smislu točke 8 člena 3 Uredbe (EU) 2018/1725 v zvezi z obdelavo osebnih podatkov s strani centralne enote ETIAS;
  - (b) so organi držav članic, ki dodajajo ali spreminjajo podatke v dokumentaciji o potrditvi identitete, upravljavci v skladu s točko 7 člena 4 Uredbe (EU) 2016/679 ali točko 8 člena 3 Direktive (EU) 2016/680 in so odgovorni za obdelavo osebnih podatkov v MID.

4. Za namene spremljanja varstva podatkov, vključno s preverjanjem dopustnosti poizvedbe in zakonitosti obdelave podatkov, imajo upravljavci podatkov dostop do dnevnikov iz členov 10, 16, 24 in 36 za notranje spremljanje iz člena 44.

#### Člen 41

#### **Obdelovalec podatkov**

V zvezi z obdelavo osebnih podatkov v skupni BMS, CIR in MID je eu-LISA obdelovalec podatkov v smislu točke 12(a) člena 3 Uredbe (EU) 2018/1725.

#### Člen 42

#### **Varnost obdelave**

1. eu-LISA, centralna enota ETIAS, Europol in organi držav članic zagotovijo varnost obdelave osebnih podatkov, ki se opravi na podlagi te uredbe. eu-LISA, centralna enota ETIAS, Europol in organi držav članic sodelujejo pri nalogah, povezanih z varnostjo.

2. Brez poseganja v člen 33 Uredbe (EU) 2018/1725 eu-LISA sprejme potrebne ukrepe za zagotovitev varnosti sestavnih delov interoperabilnosti in z njimi povezane komunikacijske infrastrukture.

3. eu-LISA zlasti sprejme potrebne ukrepe, vključno z varnostnim načrtom, načrtom neprekinjenega delovanja in sanacijskim načrtom po nesreči, za:

- (a) fizično zaščito podatkov, med drugim z izdelavo načrtov ukrepov za zaščito ključne infrastrukture ob nepredvidljivih dogodkih;
- (b) zavrnitev dostopa nepooblaščenim osebam do opreme in objektov za obdelavo podatkov;
- (c) preprečevanje nepooblaščenega branja, prepisovanja, spreminjanja ali odstranjevanja nosilcev podatkov;
- (d) preprečevanje nepooblaščenega vnosa podatkov in nedovoljenega preverjanja, spreminjanja ali brisanja zabeleženih osebnih podatkov;
- (e) preprečevanje nepooblaščenega obdelave podatkov in kakršnega koli nepooblaščenega prepisovanja, spreminjanja ali brisanja podatkov;
- (f) preprečevanje, da bi nepooblaščen osebe prek opreme za prenos podatkov uporabljale sisteme za samodejno obdelavo podatkov;
- (g) zagotovitev, da imajo osebe, pooblaščen za dostop do sestavnih delov interoperabilnosti, dostop le do podatkov, na katere se nanaša njihovo pooblastilo za dostop, na podlagi individualne uporabniške identitete ter zaupnega načina dostopa;
- (h) zagotovitev možnosti preverjanja in ugotavljanja, katerim organom se lahko z uporabo opreme za prenos podatkov posredujejo osebni podatki;
- (i) zagotovitev možnosti preverjanja in ugotavljanja, kateri podatki so bili obdelani v sestavnih delih interoperabilnosti ter kdo jih je obdeloval, kdaj in za kateri namen;
- (j) preprečevanje nepooblaščenega branja, prepisovanja, spreminjanja ali brisanja osebnih podatkov med njihovim prenosom v sestavne dele interoperabilnosti ali iz njih ali med prenosom nosilcev podatkov, zlasti z ustreznimi tehnikami šifriranja;
- (k) zagotovitev, da je v primeru prekinitve mogoče ponovno vzpostaviti normalno delovanje nameščenih sistemov;
- (l) zagotovitev zanesljivosti z ustreznim poročanjem o morebitni napaki v delovanju sestavnih delov interoperabilnosti;
- (m) spremljanje učinkovitosti varnostnih ukrepov iz tega odstavka in sprejetje potrebnih organizacijskih ukrepov v zvezi z notranjim spremljanjem, da se zagotovi skladnost s to uredbo in da se ti varnostni ukrepi ocenijo ob upoštevanju novega tehnološkega razvoja.

4. Države članice, Europol in centralna enota ETIAS v zvezi z varnostjo glede obdelave osebnih podatkov, ki jo izvajajo organi, ki imajo pravico do dostopa do katerega koli sestavnega dela interoperabilnosti, sprejmejo ukrepe, enakovredne tistim iz odstavka 3.

## Člen 43

**Varnostni incidenti**

1. Kot varnostni incident se šteje vsak dogodek, ki vpliva ali bi lahko vplival na varnost sestavnih delov interoperabilnosti in bi lahko povzročil poškodovanje ali izgubo v njih shranjenih podatkov, zlasti v primeru morebitnega nepooblaščenega dostopa do podatkov ali kadar so bile ali bi lahko bile ogrožene razpoložljivost, celovitost in zaupnost podatkov.

2. Varnostni incidenti se obvladujejo tako, da se zagotovi hiter, učinkovit in ustrezen odziv.

3. Brez poseganja v uradna obvestila in sporočila o kršitvi varstva osebnih podatkov v skladu s členom 33 Uredbe (EU) 2016/679, členom 30 Direktive (EU) 2016/680 ali obema državi članici o morebitnih varnostnih incidentih brez odlašanja obvestijo Komisijo, eu-LISA, pristojne nadzorne organe in Evropskega nadzornika za varstvo podatkov.

Brez poseganja v člena 34 in 35 Uredbe (EU) 2018/1725 ter člen 34 Uredbe (EU) 2016/794 centralna enota ETIAS in Europol o morebitnih varnostnih incidentih brez odlašanja uradno obvestita Komisijo, eu-LISA in Evropskega nadzornika za varstvo podatkov.

V primeru varnostnega incidenta, povezanega s centralno infrastrukturo sestavnih delov interoperabilnosti, eu-LISA brez odlašanja uradno obvesti Komisijo in Evropskega nadzornika za varstvo podatkov.

4. Informacije o varnostnem incidentu, ki vpliva ali bi lahko vplival na delovanje sestavnih delov interoperabilnosti ali na razpoložljivost, celovitost in zaupnost podatkov, se brez odlašanja zagotovijo državam članicam, centralni enoti ETIAS in Europolu ter se o njih poroča v skladu z načrtom za obvladovanje incidentov, ki ga zagotovi eu-LISA.

5. Države članice, ki jih incident zadeva, ter centralna enota ETIAS, Europol in eu-LISA v primeru varnostnega incidenta sodelujejo. Komisija z izvedbenimi akti določi podrobnosti tega postopka sodelovanja. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 70(2).

## Člen 44

**Notranje spremljanje**

Države članice in ustrezne agencije Unije zagotovijo, da vsak organ s pravico dostopa do sestavnih delov interoperabilnosti sprejme ukrepe, potrebne za spremljanje njegove skladnosti s to uredbo, in da po potrebi sodeluje z nadzornim organom.

Upravitelji podatkov, kakor so navedeni v členu 40, sprejmejo potrebne ukrepe za nadzor nad skladnostjo obdelave podatkov s to uredbo, vključno s pogostim preverjanjem dnevnikov iz členov 10, 16, 24 in 36, ter po potrebi sodelujejo z nadzornimi organi in z Evropskim nadzornikom za varstvo podatkov.

## Člen 45

**Kazni**

Države članice zagotovijo, da se vsaka zloraba podatkov, obdelava podatkov ali izmenjava podatkov, ki je v nasprotju s to uredbo, kaznuje v skladu z nacionalnim pravom. Kazni, ki se določijo, morajo biti učinkovite, sorazmerne in odvračilne.

## Člen 46

**Odgovornost**

1. Brez poseganja v pravico do pridobitve odškodnine od upravitelja ali obdelovalca in v njuno odgovornost na podlagi Uredbe (EU) 2016/679, Direktive (EU) 2016/680 in Uredbe (EU) 2018/1725:

- (a) je vsaka oseba ali država članica, ki je utrpela premoženjsko ali nepremoženjsko škodo zaradi nezakonitega postopka obdelave osebnih podatkov, ki ga je izvedla država članica, ali katerega koli drugega dejanja države članice, ki je v neskladju s to uredbo, upravičena do odškodnine od te države članice;

- (b) je vsaka oseba ali država članica, ki je utrpela premoženjsko ali nepremoženjsko škodo zaradi katerega koli dejanja Europol, Evropske agencije za mejno in obalno stražo ali eu-LISA, ki je v neskladju s to uredbo, upravičena do odškodnine od zadevne agencije.

Zadevna država članica, Europol, Evropska agencija za mejno in obalno stražo ali eu-LISA so v celoti ali delno oproščeni odgovornosti iz prvega pododstavka, če dokažejo, da niso odgovorni za dogodek, ki je povzročil škodo.

2. Če kakršno koli neizpolnjevanje obveznosti države članice iz te uredbe povzroči škodo sestavnim delom interoperabilnosti, je ta država članica odgovorna za tako škodo, razen če in kolikor eu-LISA ali druga država članica, ki jo zavezuje ta uredba, ni sprejela razumih ukrepov za preprečitev tovrstne škode ali zmanjšanje njenega vpliva.

3. Odškodninske zahtevke, naslovljene na državo članico zaradi škode iz odstavkov 1 in 2, ureja nacionalno pravo tožene države članice. Za odškodninske zahtevke, naslovljene na upravljavca ali eu-LISA zaradi škode iz odstavkov 1 in 2, veljajo pogoji iz Pogodb.

#### Člen 47

### Pravica do obveščenosti

1. Organ, ki zbira osebne podatke, ki se shranijo v skupni BMS, CIR ali MID, osebam, katerih podatki se zbirajo, zagotovi informacije, zahtevane v skladu s členoma 13 in 14 Uredbe (EU) 2016/679, členoma 12 in 13 Direktive (EU) 2016/680 ter členoma 15 in 16 Uredbe (EU) 2018/1725. Organ informacije zagotovi takrat, ko se zbirajo podatki o njih.

2. Vse informacije se zagotovijo v jasnem in preprostem jeziku v jezikovni različici, ki jo zadevna oseba razume ali za katero se lahko upravičeno pričakuje, da jo razume. Prav tako se osebam, na katere se nanašajo podatki in so mladoletne, informacije zagotovijo na način, ki je primeren njihovi starosti.

3. Pravila o pravici do obveščenosti iz veljavnih pravil prava unije o varstvu podatkov se uporabljajo za osebne podatke, evidentirane v sistemu ECRIS-TCN in obdelane za namene te uredbe.

#### Člen 48

### Pravica do dostopa, popravka in izbrisa osebnih podatkov, shranjenih v MID, ter omejitve njihove obdelave

1. Za uresničevanje pravic iz členov 15 do 18 Uredbe (ES) 2016/679, členov 17 do 20 Uredbe (EU) 2018/1725 ter členov 14, 15 in 16 Direktive (EU) 2016/680 ima vsaka oseba pravico, da se obrne na pristojni organ katere koli države članice, ki prouči zahtevo in nanjo odgovori.

2. Država članica, ki je prouči tako zahtevo, odgovori brez nepotrebnega odlašanja, v vsakem primeru pa v 45 dneh od prejema zahteve. Ta rok se lahko po potrebi podaljša za 15 dni ob upoštevanju kompleksnosti in števila zahtev. Država članica, ki je prouči zahtevo, obvesti posameznika, na katerega se nanašajo osebni podatki, o vsakem takem podaljšanju v 45 dneh po prejemu zahteve skupaj z razlogi za zamudo. Države članice se lahko odločijo, da morajo te odgovore podati centralni uradi.

3. Če je zahteva za popravek ali izbris osebnih podatkov vložena pri državi članici, ki ni država članica, pristojna za ročno preverjanje različnih identitet, država članica, pri kateri je bila zahteva vložena, v sedmih dneh vzpostavi stik z organi države članice, pristojne za ročno preverjanje različnih identitet. Država članica, pristojna za ročno preverjanje različnih identitet, brez nepotrebnega odlašanja, v vsakem primeru pa v 30 dneh od takega stika preveri točnost podatkov in zakonitost obdelave podatkov. Ta rok se lahko po potrebi podaljša za 15 dni ob upoštevanju kompleksnosti in števila zahtev. Država članica, pristojna za ročno preverjanje različnih identitet, obvesti državo članico, ki je vzpostavila stik, o vsakem takem podaljšanju skupaj z razlogi za zamudo. Država članica, ki je vzpostavila stik z organom države članice, pristojne za ročno preverjanje različnih identitet, zadevno osebo obvesti o nadaljnjem postopku.

4. Če je zahteva za popravek ali izbris osebnih podatkov vložena pri državi članici, kjer je bila za ročno preverjanje različnih identitet pristojna centralna enota ETIAS, država članica, pri kateri je bila zahteva vložena, v sedmih dneh vzpostavi stik s centralno enoto ETIAS in jo prosi za mnenje. Centralna enota ETIAS poda mnenje brez nepotrebne odlašanja, v vsakem primeru pa v 30 dneh od stika. Ta rok se lahko po potrebi podaljša za 15 dni ob upoštevanju kompleksnosti in števila zahtev. Država članica, ki je obvestila centralno enoto ETIAS, zadevno osebo obvesti o nadaljnjem postopku.
5. Kadar se po pregledu ugotovi, da so podatki, shranjeni v MID, netočni ali da so bili evidentirani nezakonito, država članica, pristojna za ročno preverjanje različnih identitet, ali kadar za ročno preverjanje različnih identitet ni bila pristojna nobena država članica oziroma je bila za ročno preverjanje različnih identitet pristojna centralna enota ETIAS, država članica, pri kateri je bila zahteva vložena, brez nepotrebne odlašanja popravi ali izbriše podatke. Zadevna oseba se pisno obvesti, da so bili njeni podatki popravljeni ali izbrisani.
6. Kadar država članica podatke, ki so shranjeni v MID, spremeni med njihovim obdobjem veljavnosti, izvede obdelavo iz člena 27 in, kadar je ustrezno, člena 29, da se ugotovi, ali naj se spremenjeni podatki povežejo. Če obdelava ne privede do ujemanja, ta država članica podatke izbriše iz dokumentacije o potrditvi identitete. Kadar samodejna obdelava privede do enega ali več ujemanj, ta država članica ustvari ali posodobi ustrezno povezavo v skladu z ustreznimi določbami te uredbe.
7. Kadar se država članica, pristojna za ročno preverjanje različnih identitet, ali po potrebi država članica, pri kateri je bila zahteva vložena, ne strinja, da so podatki, shranjeni v MID, netočni ali da so bili evidentirani nezakonito, ta država članica sprejme upravno odločbo, v kateri zadevni osebi nemudoma pisno pojasni razloge za nestrinjanje s popravkom ali izbrisom podatkov, ki se nanašajo nanjo.
8. Odločba iz odstavka 7 zadevni osebi zagotovi tudi informacije o možnosti izpodbijanja odločitve, sprejete v zvezi z zahtevo za dostop do popravkov, izbris ali omejitev obdelave osebnih podatkov, ter po potrebi informacije o tem, kako vložiti tožbo ali pritožbo pri pristojnih organih ali sodiščih, in o vsakršni pomoči, vključno s pomočjo nadzornih organov.
9. Vsaka zahteva za dostop do popravkov, izbris ali omejitev obdelave osebnih podatkov vsebuje potrebne informacije za identifikacijo zadevne osebe. Te informacije se uporabijo izključno zaradi uresničevanja pravic iz tega člena in se takoj po uporabi izbrišejo.
10. Država članica, odgovorna za ročno preverjanje različnih identitet, ali po potrebi država članica, pri kateri je bila zahteva vložena, vodi pisno evidenco o tem, da je bila podana zahteva za dostop do popravkov, izbris ali omejitev obdelave osebnih podatkov in kako je bila obravnavana, ter to evidenco brez odlašanja da na voljo nadzornim organom.
11. Ta člen ne posega v omejitve pravic iz tega člena v skladu z Uredbo (EU) 2016/679 in Direktivi (EU) 2016/680.

#### Člen 49

#### Spletni portal

1. Za olajšanje uveljavljanja pravice do dostopa do popravka, izbrisa ali omejitve obdelave osebnih podatkov se vzpostavi spletni portal.
2. Spletni portal vsebuje informacije o pravicah in postopkih iz členov 47 in 48 ter uporabniški vmesnik, ki osebam, katerih podatki se obdelujejo v MID in so bile obveščene o obstoju rdeče povezave v skladu s členom 32(4), omogoča prejemanje kontaktnih podatkov pristojnega organa države članice, pristojne za ročno preverjanje različnih identitet.
3. Za pridobitev kontaktnih podatkov pristojnega organa države članice, pristojnega za ročno preverjanje različnih identitet, bi morala oseba, katere podatki se obdelujejo v MID, vnesti sklic na organ, pristojen za ročno preverjanje različnih identitet, iz člena 34(d). Spletni portal uporabi ta sklic za pridobitev kontaktnih podatkov pristojnega organa države članice, pristojne za ročno preverjanje različnih identitet. Spletni portal vsebuje tudi vzorec elektronskega sporočila za lažjo komunikacijo med uporabnikom portala in pristojnim organom države članice, pristojne za ročno preverjanje različnih identitet. Takšno elektronsko sporočilo vključuje polje za enotno identifikacijsko številko iz člena 34(c), kar pristojnemu organu države članice, pristojne za ročno preverjanje različnih identitet, omogoči identifikacijo zadevnih podatkov.

4. Države članice eu-LISA zagotovijo kontaktne podatke vseh organov, pristojnih za preučitev in odgovor na katero koli zahtevo iz členov 47 in 48, ter redno pregledujejo, ali so ti kontaktni podatki posodobljeni.
5. Spletni portal razvija in tehnično upravlja eu-LISA.
6. Komisija sprejme delegirani akt v skladu s členom 69 za določitev podrobnih pravil o delovanju spletnega portala, vključno z uporabniškim vmesnikom, jeziki, v katerih je na voljo spletni portal, ter z vzorcem elektronskega sporočila.

#### Člen 50

#### **Pošiljanje osebnih podatkov tretjim državam, mednarodnim organizacijam in zasebnim subjektom**

Brez poseganja v člen 31 Uredbe (ES) št. 767/2008, člena 25 in 26 Uredbe (EU) 2016/794, člen 41 Uredbe (EU) 2017/2226, člen 65 Uredbe (EU) 2018/1240 in poizvedovanje v Interpolovih podatkovnih zbirkah prek ESP v skladu s členom 9(5) te uredbe, ki upoštevajo določbe Poglavja V Uredbe (EU) 2018/1725 in Poglavja V Uredbe (EU) 2016/679, se osebni podatki, ki so v sestavnih delih interoperabilnosti shranjeni ali jih ti obdelujejo ali do njih dostopajo, ne smejo posredovati ali dajati na voljo tretjim državam, mednarodnim organizacijam ali zasebnim subjektom.

#### Člen 51

#### **Nadzor, ki ga izvajajo nadzorni organi**

1. Vsaka država članica zagotovi, da nadzorni organi neodvisno spremljajo zakonitost obdelave osebnih podatkov na podlagi te uredbe, ki jo izvaja zadevna država članica, vključno s prenosom podatkov v sestavne dele interoperabilnosti in iz njih.
2. Vsaka država članica zagotovi, da se nacionalni zakoni in drugi predpisi, sprejeti na podlagi Direktive (EU) 2016/680, kadar je to ustrezno, uporabljajo tudi za dostop policijskih organov in imenovanih organov do sestavnih delov interoperabilnosti, tudi glede pravic oseb, do podatkov katerih se dostopa.
3. Nadzorni organi zagotovijo, da se vsaj vsaka štiri leta za namene te uredbe izvede revizija postopkov obdelave osebnih podatkov s strani odgovornih nacionalnih organov v skladu z ustreznimi mednarodnimi revizijskimi standardi.

Nadzorni organi letno objavijo število zahtev za popravek, izbris ali omejitev obdelave osebnih podatkov, ukrepov, ki so temu sledili, in število popravkov, izbrisov in omejitev obdelave, izvedenih na podlagi zahtev zadevnih oseb.

4. Države članice svojim nadzornim organom zagotovijo zadostna sredstva in strokovno znanje za opravljanje nalog, ki so jim poverjene v skladu s to uredbo.
5. Države članice nadzornemu organu iz člena 51(1) Uredbe (EU) 2016/679 zagotovijo vse informacije, ki jih ta zahteva, zlasti informacije o dejavnostih, ki se izvajajo v skladu z njihovimi odgovornostmi na podlagi te uredbe. Države članice nadzornim organom iz člena 51(1) Uredbe (EU) 2016/679 omogočijo dostop do svojih dnevnikov iz členov 10, 16, 24 in 36 te uredbe, do utemeljitev iz člena 22(2) te uredbe, in jim kadar koli dovolijo vstop v vse svoje prostore, ki se uporabljajo za namene interoperabilnosti.

#### Člen 52

#### **Revizije, ki jih izvaja Evropski nadzornik za varstvo podatkov**

Evropski nadzornik za varstvo podatkov zagotovi, da se vsaj vsaka štiri leta za namene te uredbe izvede revizija operacij eu-LISA, centralne enote ETIAS in Europol v zvezi z obdelavo osebnih podatkov v skladu z ustreznimi mednarodnimi revizijskimi standardi. Poročilo o tej reviziji se pošlje Evropskemu parlamentu, Svetu, eu-LISA, Komisiji, državam članicam in zadevni agenciji Unije. eu-LISA, centralna enota ETIAS in Europol imajo možnost, da pred sprejetjem poročil podajo pripombe.

eu-LISA, centralna enota ETIAS in Europol Evropskemu nadzorniku za varstvo podatkov zagotovijo zahtevane informacije, mu omogočijo dostop do vseh dokumentov, ki jih zahteva, in svojih dnevnikov iz členov 10, 16, 24 in 36, ter mu kadar koli dovolijo vstop v vse svoje prostore.

## Člen 53

**Sodelovanje med nadzornimi organi in Evropskim nadzornikom za varstvo podatkov**

1. Nadzorni organi in Evropski nadzornik za varstvo podatkov na področju svojih pristojnosti aktivno sodelujejo pri opravljanju svojih nalog in zagotavljajo usklajen nadzor nad uporabo sestavnih delov interoperabilnosti ter izvajanjem drugih določb te uredbe, zlasti če Evropski nadzornik za varstvo podatkov ali nadzorni organ ugotovi večja neskladja med praksami držav članic ali morebitne nezakonite prenose z uporabo komunikacijskih kanalov sestavnih delov interoperabilnosti.
2. V primerih iz odstavka 1 tega člena se zagotovi usklajen nadzor v skladu s členom 62 Uredbe (EU) 2018/1725.
3. Evropski odbor za varstvo podatkov v skladu s tem členom do 12. junija 2021 in nato vsaki dve leti Evropskemu parlamentu, Svetu, Komisiji, Europolu, Evropski agenciji za mejno in obalno stražo ter eu-LISA pošlje skupno poročilo o svojih dejavnostih na podlagi tega člena. To poročilo vsebuje poglavje o vsaki državi članici, ki ga pripravi nadzorni organ zadevne države članice.

**POGLAVJE VIII****Pristojnosti**

## Člen 54

**Pristojnosti eu-LISA med fazo zasnove in razvoja**

1. eu-LISA zagotovi, da centralne infrastrukture sestavnih delov interoperabilnosti delujejo v skladu s to uredbo.
2. Sestavne dele interoperabilnosti gosti eu-LISA na svojih tehničnih lokacijah in zagotavljajo funkcionalnosti iz te uredbe v skladu s pogoji glede varnosti, razpoložljivosti, kakovosti in učinkovitosti, navedenimi v členu 55(1).
3. eu-LISA je odgovorna za oblikovanje in razvoj sestavnih delov interoperabilnosti in za vsakršne prilagoditve, potrebne za vzpostavitev interoperabilnosti centralnih sistemov SVI, VIS, ETIAS, SIS, sistema Eurodac ter sistema ECRIS-TCN in ESP, skupne BMS, CIR, MID ter CRRS.

Brez poseganja v člen 62 eu-LISA nima dostopa do osebnih podatkov, ki se obdelujejo prek ESP, skupne BMS, CIR ali MID.

eu-LISA določi zasnovo fizične arhitekture sestavnih delov interoperabilnosti, vključno z njihovo komunikacijsko infrastrukturo, ter tehnične specifikacije in njihov razvoj glede centralne infrastrukture ter varne komunikacijske infrastrukture, ki jih sprejme upravni odbor na podlagi pozitivnega mnenja Komisije. eu-LISA izvede tudi morebitne prilagoditve SIS, sistema Eurodac ali sistema ECRIS-TCN, ki so potrebne zaradi vzpostavitve interoperabilnosti in določene s to uredbo.

eu-LISA razvije in vzpostavi sestavne dele interoperabilnosti čim prej po začetku veljavnosti te uredbe in sprejetju ukrepov iz členov 8(2), 9(7), 28(5) in (7), 37(4), 38(3), 39(5), 43(5) ter 74(10) s strani Komisije.

Razvoj zajema pripravo in izvajanje tehničnih specifikacij, preskušanje ter splošno vodenje in usklajevanje projektov.

4. Med fazo zasnove in razvoja se ustanovi Odbor za upravljanje programa z največ desetimi člani. Sestavlja ga sedem članov, ki jih izmed svojih članov ali nadomestnih članov imenuje upravni odbor eu-LISA, predsednik svetovalne skupine za interoperabilnost iz člena 71, en član, ki zastopa eu-LISA in ga imenuje njen izvršni direktor, in en član, ki ga imenuje Komisija. Člani, ki jih imenuje upravni odbor eu-LISA, se izberejo med tistimi državami članicami, za katere so po pravu Unije pravni instrumenti, ki urejajo razvoj, vzpostavitev, delovanje in uporabo vseh informacijskih sistemov EU, v celoti zavezujoči in ki bodo sodelovale pri sestavnih delih interoperabilnosti.

5. Odbor za upravljanje programa se sestaja redno in vsaj trikrat v četrtletju. Zagotovi ustrezno upravljanje faze zasnove in razvoja sestavnih delov interoperabilnosti.

Odbor za upravljanje programa upravnemu odboru eu-LISA vsak mesec predloži pisna poročila o napredku pri projektu. Odbor za upravljanje programa nima nobene pristojnosti za sprejemanje odločitev ali pooblastil za zastopanje članov upravnega odbora eu-LISA.

6. Upravni odbor eu-LISA določi poslovnik Odbora za upravljanje programa, ki vključuje zlasti pravila o:

- (a) predsedovanju;
- (b) krajih sej;
- (c) pripravi sej;
- (d) sprejemu strokovnjakov na seje;
- (e) komunikacijskih načrtih, ki zagotavljajo popolno obveščenost držav članic, ki ne sodelujejo v upravnem odboru.

Predseduje država članica, za katero so po pravu Unije pravni instrumenti, ki urejajo razvoj, vzpostavitev, delovanje in uporabo vseh informacijskih sistemov EU, v celoti zavezujoči, in ki sodelujejo v sestavnih delih interoperabilnosti.

Vse potne stroške in dnevnice članov Odbora za upravljanje programa krije eu-LISA, pri čemer se smiselno uporablja člen 10 Poslovnika eu-LISA. Sekretariat Odboru za upravljanje programa zagotovi eu-LISA.

Svetovalna skupina za interoperabilnost iz člena 71 se redno sestaja do začetka delovanja sestavnih delov interoperabilnosti. Po vsakem sestanku poroča Odboru za upravljanje programa. Zagotavlja tehnično strokovno znanje za pomoč pri nalogah Odbora za upravljanje programa in spremlja pripravljenost držav članic.

#### Člen 55

#### **Pristojnosti eu-LISA po začetku delovanja**

1. Po začetku delovanja vsakega posameznega sestavnega dela interoperabilnosti je eu-LISA pristojna za tehnično upravljanje centralne infrastrukture sestavnih delov interoperabilnosti, vključno z njihovim vzdrževanjem in tehnološkim razvojem. V sodelovanju z državami članicami zagotovi, da se uporablja najboljša razpoložljiva tehnologija na podlagi analize stroškov in koristi. eu-LISA je pristojna tudi za tehnično upravljanje komunikacijske infrastrukture iz členov 6, 12, 17, 25 in 39.

Tehnično upravljanje sestavnih delov interoperabilnosti v skladu s to uredbo obsega vse naloge in tehnične rešitve, ki so potrebne za delovanje sestavnih delov interoperabilnosti in zagotavljanje neprekinjenih storitev državam članicam in agencijam Unije 24 ur na dan in 7 dni v tednu. Vključuje vzdrževalna dela in tehnični razvoj, ki so potrebni za zagotovitev zadovoljive ravni tehnične kakovosti delovanja sestavnih delov, predvsem glede odzivnega časa, ki je potreben za iskanje po centralnih infrastrukturah, v skladu s tehničnimi specifikacijami.

Vsi sestavni deli interoperabilnosti se razvijejo in upravljajo tako, da zagotavljajo hiter, nemoten, učinkovit in nadzorovan dostop, popolno in neprekinjeno razpoložljivost sestavnih delov in podatkov, shranjenih v MID, skupni BMS in CIR, in odzivni čas, ki ustreza operativnim potrebam organov držav članic.

2. Ne glede na člen 17 Kadrovskih predpisov za uradnike Evropske unije eu-LISA za svoje osebe, ki dela s podatki, shranjenimi v sestavnih delih interoperabilnosti, uporablja ustrezna pravila glede poklicne skrivnosti ali druge enakovredne obveznosti glede zaupnosti. Ta obveznost velja tudi po tem, ko navedene osebe zapustijo delovno mesto ali prekinejo delovno razmerje, ali po prenehanju njihovih dejavnosti.

Brez poseganja v člen 62 eu-LISA nima dostopa do osebnih podatkov, ki se obdelujejo prek ESP, skupne BMS, CIR in MID.

3. eu-LISA razvije in vzdržuje mehanizem in postopke za preverjanje kakovosti podatkov, shranjenih v skupni BMS in CIR, v skladu s členom 37.

4. eu-LISA izvaja tudi naloge, povezane z zagotavljanjem usposabljanja o tehnični uporabi sestavnih delov interoperabilnosti.

## Člen 56

**Pristojnosti držav članic**

1. Vsaka država članica je pristojna za:
  - (a) povezavo s komunikacijsko infrastrukturo ESP in CIR;
  - (b) povezovanje obstoječih nacionalnih sistemov in infrastruktur z ESP, CIR ter MID;
  - (c) organizacijo, upravljanje, delovanje in vzdrževanje svoje obstoječe nacionalne infrastrukture in njene povezave s sestavnimi deli interoperabilnosti;
  - (d) upravljanje in ureditev dostopa ustrezno pooblaščenega osebja pristojnih nacionalnih organov do ESP, CIR in MID v skladu s to uredbo ter za vzpostavitev in redno posodabljanje seznama takega osebja in njegovih profilov;
  - (e) sprejetje zakonodajnih ukrepov iz člena 20(5) in (6) za dostopanje do CIR za namene identifikacije;
  - (f) ročno preverjanje različnih identitet iz člena 29;
  - (g) skladnost z zahtevami glede kakovosti podatkov, določenih v pravu Unije;
  - (h) skladnost s pravili posameznih informacijskih sistemov EU v celoti glede varnosti in celovitosti osebnih podatkov;
  - (i) odpravo vseh pomanjkljivosti, ugotovljenih v poročilu Komisije o oceni v zvezi s kakovostjo podatkov iz člena 37(5).
2. Vse države članice povežejo svoje imenovane organe s CIR.

## Člen 57

**Pristojnosti Europol**

1. Europol zagotovi obdelavo poizvedb v podatkih Europol prek ESP. Europol ustrezno prilagodi svoj vmesnik za poizvedovanje v sistemih Europol (Querying Europol Systems – QUEST) za podatke z osnovno stopnjo zaščite.
2. Europol je odgovoren za upravljanje in ureditev uporabe ESP in CIR ter dostopa do njiju s strani svojega ustrezno pooblaščenega osebja na podlagi te uredbe ter za vzpostavitev in redno posodabljanje seznama takega osebja in njegovih profilov.

## Člen 58

**Pristojnosti centralne enote ETIAS**

Centralna enota ETIAS je pristojna za:

- (a) ročno preverjanje različnih identitet v skladu s členom 29;
- (b) odkrivanje več identitet med podatki, ki so shranjeni v SVI, VIS, sistemu Eurodac in SIS, iz člena 65.

**POGLAVJE IX****Spremembe drugih instrumentov Unije**

## Člen 59

**Spremembe Uredbe (EU) 2018/1726**

Uredba (EU) 2018/1726 se spremeni:

- (1) člen 12 se nadomesti z naslednjim:

„Člen 12

**Kakovost podatkov**

1. Brez poseganja v odgovornosti držav članic glede podatkov, vnesenih v sisteme, ki spadajo podoperativno odgovornost Agencije, Agencija v tesnem sodelovanju s svojimi svetovalnimi skupinami za vse sisteme pod njenim operativnim upravljanjem vzpostavi samodejne mehanizme in postopke za nadzor kakovosti podatkov, skupne kazalnike kakovosti podatkov in minimalne standarde kakovosti za shranjevanje podatkov v skladu z ustreznimi določbami pravnih instrumentov, ki urejajo navedene informacijske sisteme, in določbami člena 37 uredb (EU) 2019/817 (\*) in (EU) 2019/818 (\*\*) Evropskega parlamenta in Sveta.

2. Agencija vzpostavi centralni register, ki vsebuje le anonimizirane podatke, za poročanje in statistične podatke v skladu s členom 39 uredb (EU) 2019/817 in (EU) 2019/818, za katerega veljajo posebne določbe v pravnih instrumentih, ki urejajo razvoj, vzpostavitev, delovanje in uporabo obsežnih informacijskih sistemov, ki jih upravlja Agencija.

- (\*) Uredba (EU) 2019/817 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju meja in vizumov ter spremembi uredb (ES) št. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 in (EU) 2018/1861 Evropskega parlamenta in Sveta ter Odločbe Sveta 2004/512/ES in Sklepa Sveta 2008/633/PNZ (UL L 135, 22.5.2019, str. 27).
- (\*\*) Uredba (EU) 2019/818 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju policijskega in pravosodnega sodelovanja, azila ter migracij in spremembi uredb (EU) 2018/1726, (EU) 2018/1862 ter (EU) 2019/816 (UL L 135, 22.5.2019, str. 85).“;

(2) v členu 19 se odstavek 1 spremeni:

(a) vstavi se naslednja točka:

„(eea) sprejme poročila o trenutnem stanju razvoja sestavnih delov interoperabilnosti v skladu s členom 78(2) Uredbe (EU) 2019/817 in členom 74(2) Uredbe (EU) 2019/818;“;

(b) točka (ff) se nadomesti z naslednjim:

„(ff) sprejme poročila o tehničnem delovanju SIS v skladu s členom 60(7) Uredbe (EU) 2018/1861 Evropskega parlamenta in Sveta (\*) in členom 74(8) Uredbe (EU) 2018/1862 Evropskega parlamenta in Sveta (\*\*), VIS v skladu s členom 50(3) Uredbe (ES) št. 767/2008 in členom 17(3) Sklepa 2008/633/PNZ, SVI v skladu s členom 72(4) Uredbe (EU) 2017/2226, ETIAS v skladu s členom 92(4) Uredbe (EU) 2018/1240 o sistemu ECRIS-TCN, referenčne programske opreme sistema ECRIS v skladu s členom 36(8) Uredbe (EU) 2019/816 Evropskega parlamenta in Sveta (\*\*\*) ter sestavnih delov interoperabilnosti v skladu s členom 78(3) Uredbe (EU) 2019/817 in členom 74(3) Uredbe (EU) 2019/818;

(\*) Uredba (EU) 2018/1861 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju mejnih kontrol, o spremembi Konvencije o izvajanju Schengenskega sporazuma ter o spremembi in razveljavitvi Uredbe (ES) št. 1987/2006 (UL L 312, 7.12.2018, str. 14).

(\*\*) Uredba (EU) 2018/1862 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi in razveljavitvi Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (ES) št. 1986/2006 Evropskega parlamenta in Sveta in Sklepa Komisije 2010/261/EU (UL L 312, 7.12.2018, str. 56).

(\*\*\*) Uredba (EU) 2019/816 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o vzpostavitvi centraliziranega sistema za določitev držav članic, ki imajo informacije o obsodbah državljanov tretjih držav in oseb brez državljanstva (sistem ECRIS-TCN), z namenom dopolnitve evropskega informacijskega sistema kazenskih evidenc ter o spremembi Uredbe (EU) 2018/1726 (UL L 135, 22.5.2019, str. 1).“;

(c) točka (hh) se nadomesti z naslednjim:

„(hh) sprejme formalne pripombe na poročila Evropskega nadzornika za varstvo podatkov o njegovih revizijah, ki se izvajajo na podlagi člena 56(2) Uredbe (EU) 2018/1861, člena 42(2) Uredbe (ES) št. 767/2008, člena 31(2) Uredbe (EU) št. 603/2013, člena 56(2) Uredbe (EU) 2017/2226, člena 67 Uredbe (EU) 2018/1240, člena 29(2) Uredbe (EU) 2019/816 ter člena 52 uredb (EU) 2019/817 in (EU) 2019/818, ter zagotovi ustrezno nadaljnje ukrepanje po teh revizijah;“;

(d) točka (mm) se nadomesti z naslednjim:

„(mm) zagotovi, da se vsako leto objavi seznam pristojnih organov, ki so pooblaščen za neposredno iskanje podatkov, shranjenih v SIS, v skladu s členom 41(8) Uredbe (EU) 2018/1861 in členom 56(7) Uredbe (EU) 2018/1862, skupaj s seznamom uradov nacionalnih sistemov SIS (N. SIS) in uradov SIRENE, v skladu s členom 7(3) Uredbe (EU) 2018/1861 oziroma členu 7(3) Uredbe (EU) 2018/1862, kakor tudi seznam pristojnih organov s skladu s členom 65(2) Uredbe (EU) 2017/2226, seznam pristojnih organov s skladu s členom 87(2) Uredbe (EU) 2018/1240, seznam centralnih organov s skladu s členom 34(2) Uredbe (EU) 2019/816 in seznam organov s skladu s členom 71(1) Uredbe (EU) 2019/817 ter člena 67(1) Uredbe (EU) 2019/818;“;

(3) v členu 22 se odstavek 4 nadomesti z naslednjim:

„4. Europol in Eurojust se lahko udeležujeta sej upravnega odbora kot opazovalca, kadar je na dnevnem redu vprašanje glede SIS II v povezavi z uporabo Sklepa 2007/533/PNZ.

Evropska agencija za mejno in obalno stražo se lahko udeležuje sej upravnega odbora kot opazovalka, kadar je na dnevnem redu vprašanje glede SIS v povezavi z uporabo Uredbe (EU) 2016/1624.

Europol se prav tako lahko udeležuje sej upravnega odbora kot opazovalec, kadar je na dnevnem redu vprašanje glede VIS v povezavi z uporabo Sklepa 2008/633/PNZ ali vprašanje glede sistema Eurodac v povezavi z uporabo Uredbe (EU) št. 603/2013.

Europol se prav tako lahko udeležuje sej upravnega odbora kot opazovalec, kadar je na dnevnem redu vprašanje glede SVI v povezavi z uporabo Uredbe (EU) 2017/2226 ali vprašanje glede ETIAS v povezavi z Uredbo (EU) 2018/1240.

Evropska agencija za mejno in obalno stražo se lahko udeležuje sej upravnega odbora kot opazovalka, kadar je na dnevnem redu vprašanje glede SIS v povezavi z uporabo Uredbe (EU) 2018/1240.

Eurojust, Europol in Evropsko javno tožilstvo se lahko udeležujejo sej upravnega odbora kot opazovalci, kadar je na dnevnem redu vprašanje glede Uredbe (EU) 2019/816.

Eurojust, Europol in Evropska agencija za mejno in obalno stražo se prav tako lahko udeležujejo sej upravnega odbora kot opazovalci, kadar je na dnevnem redu vprašanje glede uredb (EU) 2019/817 in (EU) 2019/818.

Upravni odbor lahko povabi na seje kot opazovalca kogar koli, čigar mnenje bi bilo lahko pomembno.“;

(4) v členu 24(3) se točka (p) nadomesti z naslednjim:

„(p) brez poseganja v člen 17 kadrovske predpise za uradnike, določitev zahtev glede zaupnosti zaradi skladnosti s členom 17 Uredbe (ES) št. 1987/2006, členom 17 Sklepa 2007/533/PNZ, členom 26(9) Uredbe (ES) št. 767/2008, členom 4(4) Uredbe (EU) št. 603/2013, členom 37(4) Uredbe (EU) 2017/2226, členom 74(2) Uredbe (EU) 2018/1240, členom 11(16) Uredbe (EU) 2019/816 in členom 55(2) uredb (EU) 2019/817 in (EU) 2019/818;“;

(5) člen 27 se spremeni:

(a) v odstavku 1 se doda naslednja točka:

„(da) svetovalna skupina za interoperabilnost;“;

(b) odstavek 3 se nadomesti z naslednjim:

„3. Europol, Eurojust in Evropska agencija za mejno in obalno stražo lahko imenujejo vsak svojega predstavnika v svetovalno skupino za SIS II.

Europol lahko imenuje svojega predstavnika v svetovalne skupine za VIS in sistem Eurodac ter SVI/ETIAS.

Evropska agencija za mejno in obalno stražo lahko imenuje svojega predstavnika tudi v svetovalno skupino za SVI/ETIAS.

Predstavnika v svetovalno skupino za sistem ECRIS-TCN lahko imenujejo tudi Eurojust, Europol ter Evropsko javno tožilstvo.

Europol, Eurojust in Evropska agencija za mejno in obalno stražo lahko imenujejo vsak svojega predstavnika v svetovalno skupino za interoperabilnost.“

## Člen 60

**Spremembe Uredbe (EU) 2018/1862**

Uredba (EU) 2018/1862 se spremeni:

(1) v členu 3 se dodajo naslednje točke:

- „(18) ‚ESP‘ pomeni evropski iskalni portal, vzpostavljen s členom 6(1) Uredbe (EU) 2019/818 Evropskega parlamenta in Sveta (\*);
- (19) ‚skupna BMS‘ pomeni skupno storitev za ugotavljanje ujemanja biometričnih podatkov, vzpostavljeno s členom 12(1) Uredbe (EU) 2019/818;
- (20) ‚CIR‘ pomeni skupno odložišče podatkov o identiteti, vzpostavljeno s členom 17(1) Uredbe (EU) 2019/818;
- (21) ‚MID‘ pomeni detektor več identitet, vzpostavljen s členom 25(1) Uredbe (EU) 2019/818.

(\*) Uredba (EU) 2019/818 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju policijskega in pravosodnega sodelovanja, azila ter migracij in spremembi uredb (EU) 2018/1726, (EU) 2018/1862 ter (EU) 2019/816 (UL L 135, 22.5.2019, str. 85).“;

(2) člen 4 se spremeni:

(a) v odstavku 1 se točki (b) in (c) nadomestita z naslednjim:

- „(b) nacionalnega sistema (N.SIS) v vsaki državi članici, ki je sestavljen iz nacionalnih podatkovnih sistemov, ki komunicirajo s centralnim SIS, vključno z vsaj enim nacionalnim ali deljenim rezervnim N.SIS;
- (c) komunikacijske infrastrukture med CS-SIS, rezervnim CS-SIS in NI-SIS (v nadaljnjem besedilu: komunikacijska infrastruktura), ki zagotavlja šifrirano navidezno omrežje, namenjeno podatkom SIS in izmenjavi podatkov med uradi SIRENE iz člena 7(2), in
- (d) varne komunikacijske infrastrukture med CS-SIS ter centralnimi infrastrukturami ESP, skupne BMS, in MID.“;

(b) dodata se naslednja odstavka:

„8. Brez poseganja v odstavke 1 do 5 se lahko podatki SIS o osebah in osebnih dokumentih iščejo tudi prek ESP.

9. Brez poseganja v odstavke 1 do 5 se lahko podatki SIS o osebah in osebnih dokumentih prenesejo tudi prek varne komunikacijske infrastrukture iz točke (d) odstavka 1. Ti prenosi so omejeni na obseg, ki je potreben za namene Uredbe (EU) 2019/818.“;

(3) v členu 7 se vstavi naslednji odstavek:

„2a. Uradi SIRENE zagotovijo tudi ročno preverjanje različnih identitet v skladu s členom 29 Uredbe (EU) 2019/818. Uradi SIRENE imajo v obsegu, ki je potreben za opravljanje te naloge, dostop do podatkov, shranjenih v CIR in MID, za namene iz členov 21 in 26 Uredbe (EU) 2019/818.“;

(4) v členu 12(1) se doda naslednji pododstavek:

„Države članice zagotovijo, da se zaradi preverjanja zakonitosti poizvedb, spremljanja zakonitosti obdelave podatkov, notranjega spremljanja ter celovitosti in varstva podatkov zabeleži tudi vsak dostop do osebnih podatkov prek ESP.“;

(5) v členu 44(1) se doda naslednja točka:

„(f) preverjanje različnih identitet in boj proti identitetnim prevaram v skladu s poglavjem V Uredbe (EU) 2019/818.“;

(6) v členu 74 se odstavek 7 nadomesti z naslednjim:

„7. Za namene člena 15(4) ter odstavkov 3, 4 in 6 tega člena eu-LISA hrani podatke iz člena 15(4) in odstavka 3 tega člena, ki ne smejo omogočati identifikacije posameznikov v centralnem registru za poročanje in statistične podatke iz člena 39 Uredbe (EU) 2019/818.

eu-LISA omogoči Komisiji in organom iz odstavka 6 tega člena, pridobitev prilagojenih poročil in statističnih podatkov. eu-LISA državam članicam, Komisiji, Europolu in Evropski agenciji za mejno in obalno stražo na zahtevo omogoči dostop do centralnega registra za poročanje in statistične podatke v skladu s členom 39 Uredbe (EU) 2019/818.“

#### Člen 61

### Spremembe Uredbe (EU) 2019/816

Uredba (EU) 2019/816 se spremeni:

(1) v členu 1 se doda naslednja točka:

„(c) določa pogoje, pod katerimi sistem ECRIS-TCN prispeva k olajševanju in pomoči pri pravilni identifikaciji oseb, ki so evidentirane v sistemu ECRIS-TCN, pod pogoji in za namene člena 20 Uredbe (EU) 2019/818 Evropskega parlamenta in Sveta (\*), s shranjevanjem podatkov o identiteti, podatkov o potni listini in biometričnih podatkov v CIR.

(\*) Uredba (EU) 2019/818 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju policijskega in pravosodnega sodelovanja, azila ter migracij in spremembi uredb (EU) 2018/1726, (EU) 2018/1862 ter (EU) 2019/816 (UL L 135, 22.5.2019, str. 85).“;

(2) člen 2 se nadomesti z naslednjim:

„Člen 2

#### Področje uporabe

Ta uredba se uporablja za obdelavo informacij o identiteti državljanov tretjih držav, ki so bili obsojeni v državah članicah, za namene določitve držav članic, v katerih so bile take obsodbe izrečene. Z izjemo točke (b)(ii) člena 5(1) se določbe te uredbe, ki se uporabljajo za državljane tretjih držav, uporabljajo tudi za državljane Unije, ki imajo državljanstvo tretje države in so bili obsojeni v državah članicah. Ta uredba tudi olajšuje in pomaga pri pravilni identifikaciji oseb v skladu s to uredbo in Uredbo (EU) 2019/818.“;

(3) člen 3 se spremeni:

(a) točka 8 se črta;

(b) dodajo se naslednje točke:

„(19) ‚CIR‘ pomeni skupno odložišče podatkov o identiteti, vzpostavljeno s členom 17(1) Uredbe (EU) 2019/818;

(20) ‚podatki iz sistema ECRIS-TCN‘ pomeni vse podatke, shranjene v osrednjem sistemu in v CIR v skladu s členom 5;

(21) ‚ESP‘ pomeni evropski iskalni portal, vzpostavljen s členom 6(1) Uredbe (EU) 2019/818.“;

(4) člen 4(1) se spremeni:

(a) točka (a) se nadomesti z naslednjim:

„(a) osrednji sistem;“;

(b) vstavi se naslednja točka:

„(aa) CIR;“;

(c) doda se naslednja točka:

„(e) komunikacijska infrastruktura med osrednjim sistemom ter centralnimi infrastrukturami ESP in CIR.“;

(5) člen 5 se spremeni:

(a) v odstavku 1 se uvodni del nadomesti z naslednjim:

„1. Za vsakega obsojenega državljana tretje države osrednji organ države članice izreka obsodbe ustvari podatkovni zapis v sistemu ECRIS-TCN. Podatkovni zapis vključuje:“;

(b) vstavi se naslednji odstavek:

„1a. CIR vsebuje podatke iz točke (b) odstavka 1 ter naslednje podatke iz točke (a) odstavka 1: priimek, imena, datum rojstva; kraj rojstva (mesto in država), državljanstvo ali državljanstva, spol, prejšnje ime ali imena, če je ustrezno, psevdonime ali vzdevke, kadar so na voljo, vrsto in številko potnih listin osebe ter naziv organa izdajatelja, kadar so na voljo. CIR lahko vsebuje podatke iz odstavka 3. Ostali podatki sistema ECRIS-TCN se hranijo v osrednjem sistemu.“;

(6) člen 8 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Vsak podatkovni zapis se hrani v osrednjem sistemu in CIR, dokler so podatki, ki se nanašajo na obsodbe zadevne osebe, shranjeni v kazenskih evidencah.“;

(b) odstavek 2 nadomesti z naslednjim:

„2. Po izteku obdobja hrambe iz odstavka 1 osrednji organ države članice izreka obsodbe podatkovni zapis, vključno z morebitnimi podatki o prstnih odtisih ali podobami obraza, izbriše iz osrednjega sistema in iz CIR. Izbris se po možnosti izvede samodejno, v vsakem primeru pa najpozneje v enem mesecu po izteku obdobja hrambe.“;

(7) v členu 9(1) se spremeni:

(a) v odstavku 1 se besedilo „sistem ECRIS-TCN“ v zadevnih sklonih nadomesti z besedilom „osrednji sistem in CIR“ v ustreznem sklonu;

(b) v odstavkih 2, 3 in 4 se besedilo „osrednji sistem“ v zadevnih sklonih nadomesti z besedilom „osrednji sistem in CIR“ v ustreznem sklonu;

(8) v členu 10(1) se točka (j) črta;

(9) v členu 12(2) se besedilo „osrednjem sistemu“ nadomesti z besedilom „osrednjem sistemu in v CIR“;

(10) v členu 13(2) se besedilo „osrednji sistem“ v zadevnih sklonih nadomesti z besedilom „osrednji sistem, CIR“ v ustreznem sklonu;

(11) v členu 23(2) se besedilo „osrednji sistem“ nadomesti z besedilom „osrednji sistem in v CIR“;

(12) člen 24 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Podatki, vneseni v osrednji sistem in v CIR se obdelujejo le za namene določitve držav članic, ki imajo informacije iz kazenskih evidenc državljanov tretjih držav. Podatki, vneseni v CIR, se obdelajo tudi v skladu z Uredbo (EU) 2019/818 za olajševanje in pomoč pri pravilni identifikaciji oseb, ki so evidentirane v sistemu ECRIS-TCN v skladu s to uredbo.“;

(b) doda se naslednji odstavek:

„3. Brez poseganja v odstavek 2 je dostop za namene vpogleda v podatke, shranjene v CIR, omejen na ustrezno pooblaščen osebje nacionalnih organov posameznih držav članic in na ustrezno pooblaščen osebje agencij Unije, ki so pristojni za namene iz členov 20 in 21 Uredbe (EU) 2019/818. Tak dostop je omejen na obseg, v katerem so podatki potrebni za izvajanje njihovih nalog za te namene, in sorazmeren z zasledovanimi cilji.“;

(13) v členu 32 se odstavek 2 nadomesti z naslednjim:

„2. Za namen odstavka 1 tega člena eu-LISA podatke iz navedenega odstavka hrani v centralnem registru za poročanje in statistične podatke iz člena 39 Uredbe (EU) 2019/818.“;

(14) v členu 33(1) se besedilo „osrednjega sistema“ nadomesti z besedilom „osrednjega sistema, CIR in“;

(15) v členu 41 se odstavek 2 nadomesti z naslednjim:

„2. Za obsodbe, izrečene pred datumom začetka vnašanja podatkov v skladu s členom 35(1), osrednji organi ustvarijo posamezne podatkovne zapise v osrednjem sistemu in v CIR, kakor sledi:

- (a) alfanumerični podatki se v osrednji sistem in v CIR vnesejo do konca obdobja iz člena 35(2);
- (b) podatki o prstnih odtisih se v osrednji sistem in v CIR vnesejo v dveh letih po začetku delovanja v skladu s členom 35(4).“

## POGLAVJE X

### Končne določbe

#### Člen 62

#### Poročanje in statistični podatki

1. Ustrezno pooblaščen osebje pristojnih organov držav članic, Komisije in eu-LISA ima, izključno za pripravo poročil in statistične namene, dostop do števila poizvedb na uporabnika profila ESP.

Iz podatkov ni mogoče identificirati posameznikov.

2. Ustrezno pooblaščen osebje pristojnih organov držav članic, Komisije in eu-LISA ima, izključno za pripravo poročil in statistične namene, dostop do naslednjih podatkov, povezanih s CIR:

- (a) število poizvedb za namene členov 20, 21 in 22;
- (b) državljanstvo, spol in leto rojstva osebe;
- (c) vrsta potne listine in tričrkovna oznaka države izdajateljice;
- (d) število iskanj, opravljenih z biometričnimi podatki in brez njih.

Iz podatkov ni mogoče identificirati posameznikov.

3. Ustrezno pooblaščen osebje pristojnih organov držav članic, Komisije in eu-LISA ima, izključno za pripravo poročil in statistične namene, dostop do naslednjih podatkov, povezanih z MID:

- (a) število iskanj, opravljenih z biometričnimi podatki in brez njih;
- (b) število posameznih vrst povezave in informacijski sistemi EU, ki vsebujejo povezane podatke;
- (c) obdobje, v katerem so posamezne rumene in rdeče povezave ostale v sistemu.

Iz podatkov ni mogoče identificirati posameznikov.

4. Ustrezno pooblaščen osebje Evropske agencije za mejno in obalno stražo ima pravico do vpogleda v podatke iz odstavkov 1, 2 in 3 tega člena za namene izvajanja analiz tveganj in ocen ranljivosti iz členov 11 in 13 Uredbe (EU) 2016/1624 Evropskega parlamenta in Sveta <sup>(38)</sup>.

5. Ustrezno pooblaščen osebje Europol ima pravico do vpogleda v podatke iz odstavkov 2 in 3 tega člena za namene izvajanja strateških, tematskih in operativnih analiz, kot je določeno v členu 18(2)(b) in (c) Uredbe (EU) 2016/794.

6. eu-LISA za namene odstavkov 1, 2 in 3 hrani podatke iz teh odstavkov v CRRS. Iz podatkov, vključenih v CRRS, ni mogoče identificirati posameznikov, podatki pa organom iz odstavkov 1, 2 in 3 omogočajo, da pridobijo prilagodljiva poročila in statistične podatke za izboljšanje učinkovitosti mejnih kontrol, pomoč konzulatom pri obdelavi vlog za izdajo vizuma ter podpora oblikovanju migracijske in varnostne politike Unije na podlagi dokazov.

7. Komisija Agenciji Evropske unije za temeljne pravice na zahtevo zagotovi ustrezne informacije za oceno učinka te uredbe na temeljne pravice.

<sup>(38)</sup> Uredba (EU) 2016/1624 Evropskega parlamenta in Sveta z dne 14. septembra 2016 o evropski mejni in obalni straži ter spremembi Uredbe (EU) 2016/399 Evropskega parlamenta in Sveta ter razveljavitvi Uredbe (ES) št. 863/2007 Evropskega parlamenta in Sveta, Uredbe Sveta (ES) št. 2007/2004 in Odločbe Sveta 2005/267/ES (UL L 251, 16.9.2016, str. 1).

## Člen 63

**Prehodno obdobje za uporabo evropskega iskalnega portala**

1. Obveznosti iz člena 7(2) in (4) se v obdobju dveh let po začetku delovanja ESP ne uporabljajo in uporaba ESP v tem obdobju ni obvezna.
2. Na Komisijo se prenese pooblastilo, da v skladu s členom 69 sprejeme delegirani akt, s katerim spremeni to uredbo, tako da enkrat podaljša obdobje iz odstavka 1 tega člena za največ eno leto, če je ocena praktičnega izvajanja ESP pokazala, da je takšno podaljšanje potrebno še posebej zaradi učinka, ki bi ga začetek delovanja ESP imel na organizacijo in trajanje mejnih kontrol.

## Člen 64

**Prehodno obdobje za določbe o dostopu do skupnega odložišča podatkov o identiteti za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj**

Člen 22 se uporablja od datuma začetka delovanja CIR iz člena 68(3).

## Člen 65

**Prehodno obdobje za odkrivanje več identitet**

1. V obdobju enega leta po tem, ko eu-LISA pošlje uradno obvestilo o zaključku preskusa MID iz člena 68(4)(b), in pred začetkom delovanja MID je za odkrivanje več identitet med podatki, shranjenimi v SVI, VIS, sistemu Eurodac in SIS, pristojna centralna enota ETIAS. Odkrivanje več identitet se opravlja samo z uporabo biometričnih podatkov.
2. Kadar poizvedba privede do enega ali več ujemanj in so podatki o identiteti iz povezanih dokumentacij enaki ali podobni, se vzpostavi bela povezava v skladu s členom 33.

Kadar poizvedba privede do enega ali več ujemanj in podatkov o identiteti iz povezanih dokumentacij ni mogoče šteti za podobne, se vzpostavi rumena povezava v skladu s členom 30 in se uporablja postopek iz člena 29.

V primeru več ujemanj se vzpostavi povezava med vsakim podatkom, ki je privedel do ujemanja.

3. Kadar se vzpostavi rumena povezava, MID centralni enoti ETIAS dovoli dostop do podatkov o identiteti, ki se nahajajo v različnih informacijskih sistemih EU.
4. Kadar se vzpostavi povezava na razpis ukrepa v SIS, ki ni razpis ukrepa na podlagi člena 3 Uredbe (EU) 2018/1860, členov 24 in 25 Uredbe (EU) 2018/1861 ali člena 38 Uredbe (EU) 2018/1862, MID uradu SIRENE države članice, ki je izdala razpis ukrepa, dovoli dostop do podatkov o identiteti, ki se nahajajo v različnih informacijskih sistemih.
5. Centralna enota ETIAS ali, v primerih iz odstavka 4 tega člena, urad SIRENE države članice, ki je izdala razpis ukrepa, ima dostop do podatkov v dokumentaciji o potrditvi identitete in oceni različne identitete, posodobi povezavo v skladu s členi 31, 32 in 33 ter jo doda dokumentaciji o potrditvi identitete.
6. Centralna enota ETIAS obvesti Komisijo v skladu s členom 67(3) samo, ko so bile vse rumene povezave ročno preverjene in spremenjene bodisi v zelene, bele ali rdeče povezave.
7. Centralni enoti ETIAS pri odkrivanju več identitet na podlagi tega člena po potrebi pomagajo države članice.
8. Na Komisijo se prenese pooblastilo za sprejetje delegiranega akta v skladu s členom 69 za podaljšanje obdobja iz odstavka 1 tega člena za šest mesecev, ki se lahko obnovi še dvakrat za šest mesecev. Takšno podaljšanje se odobri le po oceni predvidenega časa za izvedbo odkrivanja več identitet na podlagi tega člena, ki pokaže, da odkrivanja več identitet ne da dokončati pred iztekom preostanka roka iz odstavka 1 tega člena ali kakršnih koli tekočih podaljšanj, in da ni mogoče izvesti nobenih popravilnih ukrepov. Ocena se izvede najpozneje tri mesece pred iztekom takega roka ali tekočega podaljšanja.

**Člen 66****Stroški**

1. Stroški, ki nastanejo v zvezi z uvedbo in delovanjem ESP, skupne BMS, CIR in MID, se krijejo iz splošnega proračuna Unije.
2. Stroški, ki nastanejo v zvezi s povezovanjem obstoječih nacionalnih infrastruktur in njihovo povezavo z nacionalnimi enotnimi vmesniki ter v zvezi z gostitvijo nacionalnih enotnih vmesnikov, se krijejo iz splošnega proračuna Unije.

Izključeni so naslednji stroški:

- (a) pisarna države članice za projektno vodenje (srečanja, misije, uradi);
  - (b) gostitev nacionalnih sistemov IT (prostor, izvajanje, električna energija, hlajenje);
  - (c) delovanje nacionalnih sistemov IT (operaterji in pogodbe za izvajanje podpornih storitev);
  - (d) zasnova, razvoj, izvajanje, delovanje in vzdrževanje nacionalnih komunikacijskih omrežij.
3. Brez poseganja v nadaljnje financiranje v ta namen iz drugih virov splošnega proračuna Evropske unije se iz sredstev v višini 791 000 000 EUR, predvidenih v členu 5(5)(b) Uredbe (EU) št. 515/2014 za kritje stroškov izvajanja te uredbe, kakor je predvideno v odstavkih 1 in 2 tega člena, uporabi znesek 32 077 000 EUR.
  4. Iz sredstev iz odstavka 3 bo 22 861 000 EUR dodeljenih eu-LISA, 9 072 000 EUR bo dodeljenih Europolu, 144 000 EUR pa bo dodeljenih Agenciji Evropske unije za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Cepol) za podporo tem agencijam pri izvajanju nalog v skladu na podlagi te uredbe. To financiranje se izvaja v okviru posrednega upravljanja.
  5. Stroške imenovanih organov krijejo države članice, ki so imenovalе te organe. Stroške povezave vsakega imenovanega organa s CIR krije vsaka država članica.

Stroške Eurola, vključno s povezavo s CIR, krije Europol.

**Člen 67****Uradna obvestila**

1. Države članice eu-LISA uradno obvestijo o organih iz členov 7, 20, 21 in 26, ki lahko uporabljajo ESP, CIR oziroma MID ali imajo do njih dostop.

V treh mesecih po začetku delovanja vsakega posameznega sestavnega dela interoperabilnosti v skladu s členom 68 se v *Uradnem listu Evropske unije* objavi zbirni seznam teh organov. V primeru sprememb tega seznama eu-LISA enkrat letno objavi posodobljen zbirni seznam.

2. Agencija eu-LISA Komisijo uradno obvesti o uspešnem dokončanju preskusa iz člena 68(1)(b), (2)(b), (3)(b), (4)(b), (5)(b) in (6)(b).
3. Centralna enota ETIAS Komisijo uradno obvesti o uspešnem dokončanju prehodnega obdobja iz člena 65.
4. Komisija informacije, o katerih je uradno obveščena v skladu z odstavkom 1, državam članicam in javnosti da na voljo prek javnega spletnega mesta, ki se stalno posodablja.

**Člen 68****Začetek delovanja**

1. Komisija z izvedbenim aktom določi datum začetka delovanja ESP, ko so izpolnjeni naslednji pogoji:
  - (a) sprejeti so ukrepi iz členov 8(2), 9(7) ter 43(5);

- (b) eu-LISA objavi uspešno dokončanje celovitega preskusa ESP, ki ga je izvedla skupaj z organi država članic in agencijami Unije, ki lahko uporabljajo ESP;
- (c) eu-LISA potrdi tehnične in pravne ukrepe za zbiranje in prenos podatkov iz člena 8(1) ter o njih uradno obvesti Komisijo.

ESP opravi poizvedbo v Interpolovih podatkovnih zbirkah le, ko tehnična ureditev omogoča skladnost s členom 9(5). Vsaka neskladnost s členom 9(5) ima za posledico, da ESP ne poizveduje v Interpolovih podatkovnih zbirkah, vendar to ne odloži začetka delovanja ESP.

Komisija datum iz prvega pododstavka določi v 30 dneh od sprejetja izvedbenega akta.

2. Komisija z izvedbenim aktom določi datum začetka delovanja skupne BMS, ko so izpolnjeni naslednji pogoji:

- (a) sprejeti so ukrepi iz členov 13(5) ter 43(5);
- (b) eu-LISA objavi uspešno dokončanje celovitega preskusa skupne BMS, ki ga je izvedla skupaj z organi držav članic;
- (c) eu-LISA potrdi tehnične in pravne ukrepe za zbiranje in prenos podatkov iz člena 13 ter o njih uradno obvesti Komisijo;
- (d) eu-LISA objavi uspešno dokončanje preskusa iz odstavka 5(b).

Komisija datum iz prvega pododstavka določi v 30 dneh od sprejetja izvedbenega akta.

3. Komisija z izvedbenim aktom določi datum začetka delovanja CIR, ko so izpolnjeni naslednji pogoji:

- (a) sprejeti so ukrepi iz členov 43(5) ter 74(10);
- (b) eu-LISA objavi uspešno dokončanje celovitega preskusa CIR, ki ga je izvedla skupaj z organi držav članic;
- (c) eu-LISA potrdi tehnične in pravne ukrepe za zbiranje in prenos podatkov iz člena 18 ter o njih uradno obvesti Komisijo;
- (d) eu-LISA objavi uspešno dokončanje preskusa iz odstavka 5(b).

Komisija datum iz prvega pododstavka določi v 30 dneh od sprejetja izvedbenega akta.

4. Komisija z izvedbenim aktom določi datum začetka delovanja MID, ko so izpolnjeni naslednji pogoji:

- (a) sprejeti so ukrepi iz členov 28(5) in (7), 32(5), 33(6), 43(5) ter 49(6);
- (b) eu-LISA objavi uspešno dokončanje celovitega preskusa MID, ki ga je izvedla skupaj z organi držav članic in centralno enoto ETIAS;
- (c) eu-LISA potrdi tehnične in pravne ukrepe za zbiranje in prenos podatkov iz člena 34 ter o njih uradno obvesti Komisijo;
- (d) centralna enota ETIAS uradno obvesti Komisijo v skladu s členom 67(3);
- (e) eu-LISA objavi uspešno dokončanje preskusov iz odstavkov 1(b), 2(b), 3(b) in 5(b).

Komisija datum iz prvega pododstavka določi v 30 dneh od sprejetja izvedbenega akta.

5. Komisija z izvedbenimi akti določi datum, od katerega se uporabljajo samodejni mehanizmi in postopki za nadzor kakovosti podatkov, skupni kazalniki kakovosti podatkov in minimalni standardi kakovosti, ko so izpolnjeni naslednji pogoji:

- (a) sprejeti so ukrepi iz člena 37(4);

- (b) eu-LISA objavi uspešno dokončanje celovitega preskusa samodejnih mehanizmov in postopkov za nadzor kakovosti podatkov, skupnih kazalnikov kakovosti podatkov in minimalnih standardov kakovosti, ki ga je izvedla skupaj z organi držav članic.

Komisija datum iz prvega pododstavka določi v 30 dneh od sprejetja izvedbenega akta.

6. Komisija z izvedbenim aktom določi datum začetka delovanja CRRS, ko so izpolnjeni naslednji pogoji:

- (a) sprejeti so ukrepi iz členov 39(5) ter 43(5);
- (b) eu-LISA objavi uspešno dokončanje celovitega preskusa CRRS, ki ga je izvedla skupaj z organi držav članic;
- (c) eu-LISA potrdi tehnične in pravne ukrepe za zbiranje in prenos podatkov iz člena 39 ter o njih uradno obvesti Komisijo.

Komisija datum iz prvega pododstavka določi v 30 dneh od sprejetja izvedbenega akta.

7. Komisija obvesti Evropski parlament in Svet o rezultatih preskusov, opravljenih v skladu z odstavki 1(b), 2(b), 3(b), 4(b), 5(b) in 6(b).

8. Države članice, centralna enota ETIAS in Europol začnejo uporabljati vsakega od sestavnih delov interoperabilnosti od datuma, ki ga Komisija določi v skladu z odstavki 1, 2, 3 oziroma 4.

#### Člen 69

##### Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.
2. Pooblastilo za sprejemanje delegiranih aktov iz členov 28(5), 39(5), 49(6), 63(2) in 65(8) se prenese na Komisijo za obdobje petih let od 11. junija 2019. Komisija pripravi poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem petletnega obdobja. Prenos pooblastila se samodejno podaljšuje za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.
3. Prenos pooblastila iz členov 28(5), 39(5), 49(6), 63(2) in 65(8) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.
4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.
5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.
6. Delegirani akt, sprejet v skladu s členi 28(5), 39(5), 49(6), 63(2) in 65(8), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

#### Člen 70

##### Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.
2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

Kadar odbor ne da mnenja, Komisija osnutka izvedbenega akta ne sprejme in se uporabi tretji pododstavek člena 5(4) Uredbe (EU) št. 182/2011.

## Člen 71

**Svetovalna skupina**

eu-LISA ustanovi svetovalno skupino. V fazi zasnove in razvoja sestavnih delov interoperabilnosti se uporablja člen 54(4), (5) in (6).

## Člen 72

**Usposabljanje**

eu-LISA izvaja naloge, povezane z zagotavljanjem usposabljanja o tehnični uporabi sestavnih delov interoperabilnosti, v skladu z Uredbo (EU) 2018/1726.

Organi držav članic in agencije Unije za svoje osebje, ki je pooblaščen za obdelavo podatkov z uporabo sestavnih delov interoperabilnosti, zagotovijo ustrezen program usposabljanja o varnosti podatkov, kakovosti podatkov, pravilih varstva podatkov, postopkih, ki se uporabljajo za obdelavo podatkov, in obveznostih obveščanja na podlagi členov 32(4), 33(4) in 47.

Kadar je primerno, se organizirajo skupna usposabljanja o teh temah na ravni Unije, da se izboljša sodelovanje in izmenjava primerov dobrih praks med osebjem organov držav članic in agencij Unije, pooblaščenim za obdelavo podatkov z uporabo sestavnih delov interoperabilnosti. Posebna pozornost se nameni postopku odkrivanja več identitet, vključno z ročnim preverjanjem različnih identitet in spremljajočo potrebo, da se ohranjajo ustrezni zaščitni ukrepi v zvezi s temeljnimi pravicami.

## Člen 73

**Praktični priročnik**

Komisija v tesnem sodelovanju z državami članicami, eu-LISA in drugimi zadevnimi agencijami Unije pripravi praktični priročnik za izvajanje in upravljanje sestavnih delov interoperabilnosti. Praktični priročnik določa tehnične in operativne smernice, priporočila in dobre prakse. Komisija sprejme praktični priročnik v obliki priporočila.

## Člen 74

**Spremljanje in ocenjevanje**

1. eu-LISA zagotovi, da so vzpostavljeni postopki za spremljanje razvoja sestavnih delov interoperabilnosti in njihovega povezovanja z enotnim nacionalnim vmesnikom ob upoštevanju ciljev v zvezi z načrtovanjem in stroški ter spremljanje delovanja sestavnih delov interoperabilnosti ob upoštevanju ciljev v zvezi s tehničnimi rezultati, stroškovno učinkovitostjo, varnostjo in kakovostjo storitev.

2. eu-LISA do 12. decembra 2019 in nato vsakih šest mesecev med razvojno fazo sestavnih delov predloži Evropskemu parlamentu in Svetu poročilo o stanju razvoja posameznih sestavnih delov ter o njihovem povezovanju z enotnim nacionalnim vmesnikom. Po končanem razvoju se Evropskemu parlamentu in Svetu predloži poročilo, ki podrobno pojasnjuje, kako so bili izpolnjeni zlasti cilji, povezani z načrtovanjem in stroški, ter utemljuje morebitna odstopanja.

3. eu-LISA štiri leta po začetku delovanja vsakega posameznega sestavnega dela interoperabilnosti v skladu s členom 68 in nato vsaka štiri leta Evropskemu parlamentu, Svetu in Komisiji predloži poročilo o tehničnem delovanju sestavnih delov interoperabilnosti, vključno z njihovo varnostjo.

4. Poleg tega Komisija eno leto po vsakem poročilu eu-LISA izdela splošno oceno sestavnih delov interoperabilnosti, ki vključuje:

- (a) oceno uporabe te uredbe;
- (b) pregled doseženih rezultatov glede na zastavljene cilje te uredbe in njenih učinkov na temeljne pravice, zlasti oceno učinkov sestavnih delov interoperabilnosti na pravico do nediskriminacije;
- (c) oceno delovanja spletnega portala, vključno s podatki o uporabi spletnega portala in številom zahtevkov, ki so bili rešeni;
- (d) oceno nadaljnje ustreznosti temeljnih razlogov za sestavne dele interoperabilnosti;

- (e) oceno varnosti sestavnih delov interoperabilnosti;
- (f) oceno uporabe CIR za identifikacijo;
- (g) oceno uporabe CIR za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj;
- (h) oceno morebitnih posledic, vključno s kakršnimi koli nesorazmernimi vplivi na pretok prometa na mejnih prehodih in posledicami s proračunskim vplivom na splošni proračun Unije;
- (i) oceno iskanja po Interpolovih podatkovnih zbirkah prek ESP, vključno z informacijami o številu zadetkov v Interpolovih podatkovnih zbirkah in informacijami o vseh nastalih težavah.

Splošna ocena na podlagi prvega pododstavka tega odstavka vključuje morebitna potrebna priporočila. Komisija poročilo o oceni posreduje Evropskemu parlamentu, Svetu, Evropskemu nadzorniku za varstvo podatkov in Agenciji Evropske unije za temeljne pravice.

5. Komisija do 12. junija 2020 in nato vsako leto, dokler ne sprejme izvedbenih aktov iz člena 68, Evropskemu parlamentu in Svetu predloži poročilo o stanju priprav na celovito izvajanje te uredbe. To poročilo vsebuje tudi podrobne informacije o nastalih stroških in o morebitnih tveganjih, ki bi lahko vplivala na skupne stroške.

6. Komisija dve leti po začetku delovanja MID v skladu s členom 68(4) izvede pregled učinka MID na pravico do nediskriminacije. Po tem prvem poročilu je pregled učinka MID na pravico do nediskriminacije del pregleda iz odstavka 4(b) tega člena.

7. Države članice in Europol eu-LISA in Komisiji predložijo informacije, potrebne za pripravo poročil iz odstavkov 3 do 6. Te informacije ne smejo ogroziti delovnih metod ali vključevati informacij, ki razkrivajo vire, člane osebja ali preiskave imenovanih organov.

8. eu-LISA Komisiji predloži informacije, potrebne za pripravo skupne ocene iz odstavka 4.

9. V skladu s predpisi nacionalnega prava o objavi občutljivih informacij in brez poseganja v omejitve, potrebne za zaščito varnosti in javnega reda, preprečevanje kriminala in zagotavljanje, da nobena nacionalna preiskava ne bo ogrožena, vse države članice in Europol za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj pripravijo letna poročila o učinkovitosti dostopa do podatkov, shranjenih v CIR, ki morajo zajemati informacije in statistične podatke o:

- (a) natančnih namenih vpogledov, vključno z vrstami terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj;
- (b) razumnih razlogih za utemeljen sum, da je osumljenec, storilec ali žrtev zajet z Uredbo (EU) št. 603/2013;
- (c) številu zahtev za dostop do CIR za namene preprečevanja, odkrivanja ali preiskovanja terorističnih kaznivih dejanj ali drugih hudih kaznivih dejanj;
- (d) številu in vrsti zadev, ki so vodile do uspešne identifikacije;
- (e) potrebi in uporabi izjem za nujne primere, vključno s tistimi primeri, pri katerih se po naknadnem preverjanju, ki ga je opravila centralna točka dostopa, ta nujnost ni sprejela.

Letna poročila držav članic in Eurola se pošljejo Komisiji do 30. junija naslednjega leta.

10. Državam članicam se da na voljo tehnična rešitev za upravljanje zahtev za dostop uporabnikov iz člena 22 in olajšanje zbiranja informacij iz odstavkov 7 in 9 tega člena, za namene generiranja poročil in statističnih podatkov iz navedenih odstavkov. Komisija z izvedbenimi akti sprejme specifikacije te tehnične rešitve. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 70(2).

## Člen 75

**Začetek veljavnosti in uporaba**

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Določbe te uredbe v zvezi z ESP se uporabljajo od datuma, ki ga določi Komisija v skladu s členom 68(1).

Določbe te uredbe v zvezi s skupno BMS se uporabljajo od datuma, ki ga določi Komisija v skladu s členom 68(2).

Določbe te uredbe v zvezi s CIR se uporabljajo od datuma, ki ga določi Komisija v skladu s členom 68(3).

Določbe te uredbe v zvezi z MID se uporabljajo od datuma, ki ga določi Komisija v skladu s členom 68(4).

Določbe te uredbe v zvezi s samodejnimi mehanizmi in postopki za nadzor kakovosti podatkov, skupnimi kazalniki kakovosti podatkov ter minimalnimi standardi kakovosti podatkov se uporabljajo od datuma, ki ga določi Komisija v skladu s členom 68(5).

Določbe te uredbe v zvezi s CRRS se uporabljajo od datuma, ki ga določi Komisija v skladu s členom 68(6).

Členi 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71, 73 in 74(1) se uporabljajo od 11. junija 2019.

Ta uredba se uporablja v zvezi s sistemom Eurodac od datuma, ko se začne uporabljati prenovitev Uredbe (EU) št. 603/2013.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v državah članicah v skladu s Pogodbama.

V Bruslju, 20. maja 2019

*Za Evropski parlament*

*Predsednik*

A. TAJANI

*Za Svet*

*Predsednik*

G. CIAMBA