EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2019/818

af 20. maj 2019

om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende politisamarbejde og retligt samarbejde, asyl og migration og om ændring af forordning (EU) 2018/1726, (EU) 2018/1862 og (EU) 2019/816

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16, stk. 2, artikel 74, artikel 78, stk. 2, litra e), artikel 79, stk. 2, litra c), artikel 82, stk. 1, litra d), artikel 85, stk. 1, artikel 87, stk. 2, litra a), og artikel 88, stk. 2,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([1]),

efter høring af Regionsudvalget,

efter den almindelige lovgivningsprocedure ([2]), og

ud fra følgende betragtninger:

(1) Kommissionen understregede i sin meddelelse af 6. april 2016 med titlen Stærkere og mere intelligente informationssystemer for grænser og sikkerhed nødvendigheden af at forbedre Unionens dataforvaltningsstruktur for grænseforvaltning og sikkerhed. Meddelelsen indledte en proces med henblik på at opnå interoperabilitet mellem EU-informationssystemer for sikkerhed og grænse- og migrationsforvaltning med det formål at afhjælpe de strukturelle mangler i forbindelse med disse systemer, som hindrer de nationale myndigheders arbejde, og for at sikre, at grænsevagter, toldmyndigheder, politifolk og retslige myndigheder råder over de nødvendige oplysninger.

(2) I sin køreplan om styrkelse af informationsudveksling og informationsstyring, herunder interoperabilitetsløsninger på området for retlige og indre anliggender, af 6. juni 2016 kortlagde Rådet forskellige juridiske, tekniske og driftsmæssige udfordringer i forbindelse med EU-informationssystemernes interoperabilitet og opfordrede til at finde løsninger.

(3) Europa-Parlamentet opfordrede i sin beslutning af 6. juli 2016 om de strategiske prioriteringer for Kommissionens arbejdsprogram for 2017 ([3]) til fremlæggelse af forslag til at forbedre og udvikle eksisterende EU-informationssystemer, løse problemet med manglende oplysninger og gå i retning af interoperabilitet samt forslag om obligatorisk udveksling af oplysninger på EU-plan ledsaget af de nødvendige databeskyttelsesregler.

(4) I sine konklusioner af 15. december 2016 opfordrede Det Europæiske Råd til, at arbejdet skulle fortsætte med at levere interoperabilitet for så vidt angår EU-informationssystemer og -databaser.

(5) Ekspertgruppen på højt niveau om informationssystemer og interoperabilitet konkluderede i sin endelige rapport af 11. maj 2017, at det var nødvendigt og teknisk gennemførligt at arbejde hen imod praktiske interoperabilitetsløsninger, og at interoperabilitet i princippet både kan sikre operationelle gevinster og indføres under overholdelse af kravene om databeskyttelse.

(6) I sin meddelelse af 16. maj 2017 med titlen Syvende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion fastlagde Kommissionen i overensstemmelse med sin meddelelse af 6. april 2016 og med resultaterne og anbefalingerne fra ekspertgruppen på højt niveau om informationssystemer og interoperabilitet en ny tilgang til forvaltning af oplysninger for grænser, sikkerhed og migration, hvorefter alle EU-informationssystemer for sikkerhed, grænse- og migrationsforvaltning skulle være interoperable på en måde, der fuldt ud respekterer de grundlæggende rettigheder.

---

(1) EUT C 283 af 10.8.2018, s. 48.
(2) Europa-Parlamentets holdning af 16.4.2019 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 14.5.2019.
(3) EUT C 101 af 16.3.2018, s. 116.

(7) Rådet opfordrede i sine konklusioner af 9. juni 2017 om vejen frem for at forbedre udvekslingen af oplysninger og sikre interoperabiliteten mellem EU-informationssystemer Kommissionen til at forfølge de interoperabilitetsløsninger, som ekspertgruppen på højt niveau havde foreslået.

(8) I sine konklusioner af 23. juni 2017 understregede Det Europæiske Råd behovet for at forbedre interoperabiliteten mellem databaser og opfordrede Kommissionen til snarest muligt at udarbejde udkast til lovgivning på grundlag af de forslag, som var fremsat af ekspertgruppen på højt niveau om informationssystemer og interoperabilitet.

(9) Med henblik på at forbedre effektiviteten af kontrollen ved de ydre grænser, bidrage til at forebygge og bekæmpe ulovlig indvandring og bidrage til et højt sikkerhedsniveau inden for området med frihed, sikkerhed og retfærdighed i Unionen, herunder opretholdelsen af den offentlige sikkerhed og den offentlige orden og beskyttelse af sikkerhed på medlemsstaternes områder, forbedre implementeringen af den fælles visumpolitik, bistå ved gennemgangen af ansøgninger om international beskyttelse, bidrage til forebyggelsen, afsløringen og efterforskningen af terrorhandlinger og andre alvorlige strafbare handlinger, lette identifikationen af ukendte personer, der er ude af stand til at legitimere sig, eller uidentificerede menneskelige rester i tilfælde af en naturkatastrofe, en ulykke eller et terrorangreb, i den hensigt at bevare offentlighedens tillid til Unionens migrations- og asylsystem, Unionens sikkerhedsforanstaltninger og Unionens evne til at forvalte de ydre grænser, bør der skabes interoperabilitet mellem EU-informationssystemer, navnlig ind- og udrejsesystemet, visuminformationssystemet (VIS), det europæiske system vedrørende rejseinformation og rejsetilladelse (ETIAS), Eurodac, Schengeninformationssystemet (SIS) og det europæiske informationssystem til udveksling af oplysninger fra strafferegistre vedrørende tredjelandsstatsborgere (ECRIS-TCN), så disse EU-informationssystemer og deres oplysninger supplerer hinanden, samtidig med at individets grundlæggende rettigheder, særligt retten til beskyttelse af personoplysninger, respekteres. For at opnå dette bør der oprettes en europæisk søgeportal (ESP), en fælles biometrisk matchtjeneste (fælles BMS), et fælles identitetsregister (CIR) og en multiidentitetsdetektor (MID) som interoperabilitetskomponenter.

(10) Interoperabilitet mellem EU-informationssystemerne bør gøre det muligt for disse systemer at supplere hinanden for at lette korrekt identifikation af personer, herunder af ukendte personer, der er ude af stand til at legitimere sig, eller uidentificerede menneskelige rester, bidrage til at bekæmpe identitetssvig, forbedre og harmonisere datakvalitetskravene i de enkelte EU-informationssystemer, lette den tekniske og praktiske gennemførelse i medlemsstaterne af EU-informationssystemer, styrke datasikkerheden og de databeskyttelsesregler, der gælder for de respektive EU-informationssystemer, strømline adgang til ind- og udrejsesystemet, VIS, ETIAS og Eurodac med det formål at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger, samt støtte formålene med ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN.

(11) Interoperabilitetskomponenterne bør omfatte ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN. De bør også omfatte Europoloplysningerne, men kun i det omfang det giver mulighed for at forespørge i Europoloplysningerne samtidig med de nævnte EU-informationssystemer.

(12) Interoperabilitetskomponenterne bør behandle personoplysninger for personer, hvis personoplysninger behandles i de underliggende EU-informationssystemer og af Europol.

(13) ESP bør oprettes for at lette medlemsstatsmyndigheders og EU-agenturers hurtige, problemfri, effektive, systematiske og kontrollerede adgang til EU-informationssystemerne, Europoloplysningerne og Den Internationale Kriminalpolitiorganisations (INTERPOL's) databaser, i det omfang dette er nødvendigt for, at de kan udføre deres opgaver, i overensstemmelse med deres adgangsrettigheder. ESP bør også oprettes for at støtte formålene med ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN og Europoloplysningerne. Ved at gøre det muligt at forespørge i alle relevante EU-informationssystemer, Europoloplysningerne og INTERPOL-databaserne parallelt bør ESP fungere som en enkelt grænseflade eller »meddelelsesformidler« med hensyn til at søge i de forskellige centrale systemer og udtrække de nødvendige oplysninger problemfrit og under fuld overholdelse af de underliggende systemers krav til adgangskontrol og databeskyttelse.

(14) Udformningen af ESP bør sikre, at de oplysninger, der i forbindelse med forespørgsler i INTERPOL-databaserne anvendes af en ESP-bruger til at iværksætte en forespørgsel, ikke deles med ejerne af INTERPOL-oplysninger. Udformningen af ESP bør også sikre, at der kun foretages forespørgsler i INTERPOL-databaserne i overensstemmelse med gældende EU-ret og national ret.

(15) De ESP-brugere, som har adgangsret til Europoloplysningerne i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/794 ([4]), bør være i stand til at søge i Europoloplysningerne samtidigt med de EU-informationssystemer, som de har adgang til. Enhver yderligere databehandling efter en sådan forespørgsel bør finde sted som omhandlet i forordning (EU) 2016/794, herunder begrænsninger på adgang eller brug indført af dataleverandøren.

(16) ESP bør udvikles og konfigureres på en sådan måde, at den kun tillader sådanne forespørgsler, som anvender oplysninger vedrørende personer eller rejsedokumenter, der forefindes i et EU-informationssystem, i Europoloplysningerne eller i INTERPOL-databaserne.

(17) For at sikre systematisk brug af de relevante EU-informationssystemer bør ESP anvendes til forespørgsler i CIR, ind- og udrejsesystemet, VIS, ETIAS, Eurodac og ECRIS-TCN. En national forbindelse til de forskellige EU-informationssystemer bør dog fastholdes som et teknisk sikkerhedsnet. EU-agenturerne bør ligeledes anvende ESP til at forespørge i det centrale SIS i overensstemmelse med deres adgangsrettigheder og for at udføre deres opgaver. ESP bør være et yderligere middel til forespørgsler i det centrale SIS, Europoloplysningerne og INTERPOL-databaserne som supplement til de eksisterende specifikke grænseflader.

(18) Biometriske oplysninger såsom fingeraftryk og ansigtsbilleder er unikke og derfor meget mere pålidelige end alfanumeriske oplysninger med henblik på at identificere en person. Den fælles BMS bør være et teknisk redskab til at styrke og lette de relevante EU-informationssystemers og de andre interoperabilitetskomponenters funktion. Det vigtigste formål med den fælles BMS bør være at lette identifikationen af en person, som er registreret i adskillige databaser, ved at anvende en unik teknologisk komponent til at matche denne persons biometriske oplysninger på tværs af forskellige systemer i stedet for at anvende adskillige komponenter. Den fælles BMS bør både bidrage til sikkerheden samt give finansielle, vedligeholdelsesmæssige og driftsmæssige fordele. Alle automatiserede fingeraftryksidentifikationssystemer, herunder dem, der i øjeblikket anvendes til Eurodac, VIS og SIS, anvender biometriske skabeloner, som består af oplysninger, der udledes af træk fra faktiske biometriske prøver. Den fælles BMS bør omgruppere og lagre alle disse biometriske skabeloner — logisk adskilt efter det informationssystem, oplysningerne stammer fra — på ét enkelt sted for således at lette sammenligninger på tværs af systemer ved hjælp af biometriske skabeloner og give stordriftsfordele med hensyn til at udvikle og opretholde de centrale EU-systemer.

(19) De biometriske skabeloner, som er lagret i den fælles BMS, bør bestå af oplysninger hidrørende fra udledning af træk fra faktiske biometriske prøver og skabes på en sådan måde, at det ikke er muligt at vende udledningsprocessen om. Biometriske skabeloner bør skabes ud fra biometriske oplysninger, men det bør ikke være muligt at genskabe de samme biometriske oplysninger ud fra de biometriske skabeloner. Da håndfladeaftryksdata og DNA-profiler kun lagres i SIS og ikke kan bruges til at udføre krydstjek med oplysninger i andre informationssystemer, bør den fælles BMS i henhold til nødvendigheds- og proportionalitetsprincippet ikke opbevare DNA-profiler eller biometriske skabeloner hidrørende fra håndfladeaftryksdata.

(20) Biometriske oplysninger udgør følsomme personoplysninger. Denne forordning bør fastsætte grundlaget for og sikkerhedsforanstaltningerne ved behandling af sådanne oplysninger med det formål entydigt at identificere de berørte personer.

(21) Ind- og udrejsesystemet, VIS, ETIAS, Eurodac og ECRIS-TCN kræver nøjagtig identifikation af de personer, hvis personoplysninger er lagret i dem. CIR bør derfor lette korrekt identifikation af personer, der er registreret i disse systemer.

(22) Personoplysninger, der lagres i disse EU-informationssystemer, kan vedrøre de samme personer, men under forskellige eller ufuldstændige identiteter. Medlemsstaterne råder over effektive metoder til at identificere deres borgere eller registrerede fastboende personer på deres område. Interoperabiliteten mellem EU-informationssystemer bør bidrage til korrekt identifikation af personer, der er i disse systemer. CIR bør lagre de personoplysninger, der er nødvendige for at foretage en mere præcis identifikation af de personer, hvis oplysninger er lagret i disse systemer, herunder deres identitetsoplysninger, rejsedokumentoplysninger og biometriske oplysninger, uanset i hvilket system oplysningerne oprindeligt blev indsamlet. Kun de personoplysninger, der er strengt nødvendige for at foretage en nøjagtig identitetskontrol, bør lagres i CIR. De personoplysninger, der er registreret i CIR, bør kun opbevares så længe, det er strengt nødvendigt med henblik på de underliggende systemer, og bør slettes automatisk, når oplysningerne slettes fra de underliggende systemer i overensstemmelse med deres logiske adskillelse.

([4]) Europa-Parlamentets og Rådets forordning (EU) 2016/794 af 11. maj 2016 om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) og om erstatning og ophævelse af Rådets afgørelse 2009/371/RIA, 2009/934/RIA, 2009/935/RIA, 2009/936/RIA og 2009/968/RIA (EUT L 135 af 24.5.2016, s. 53).

(23) En ny behandlingsaktivitet, der består i at lagre sådanne oplysninger i CIR i stedet for at lagre dem i hvert af de særskilte systemer, er nødvendig for at øge nøjagtigheden af identifikation via automatiseret sammenligning og matchning af oplysninger. Den omstændighed, at identitetsoplysninger, rejsedokumentoplysninger og biometriske oplysninger lagres i CIR, bør ikke på nogen måde være til hinder for behandlingen af oplysninger med henblik på ind- og udrejsesystemet, VIS, ETIAS, Eurodac eller ECRIS-TCN, eftersom CIR vil være en ny fælles komponent for disse underliggende systemer.

(24) Det er derfor nødvendigt at oprette en individuel mappe i CIR for hver person, der registreres i ind- og udrejsesystemet, VIS, ETIAS, Eurodac eller ECRIS-TCN, for at opfylde formålet med korrekt identifikation af personer inden for Schengenområdet og for at støtte MID for det dobbelte formål at lette identitetskontrol for bona fide-rejsende og bekæmpe identitetssvig. Den individuelle mappe bør lagre alle de identitetsoplysninger, der er knyttet til en person, et enkelt sted og give alle behørigt autoriserede slutbrugere adgang dertil.

(25) CIR bør således lette og effektivisere adgangen for myndigheder med ansvar for forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger til de EU-informationssystemer, der ikke er oprettet udelukkende med henblik på forebyggelse, afsløring eller efterforskning af grov kriminalitet.

(26) CIR bør være et fælles register over identitetsoplysninger, rejsedokumentoplysninger og biometriske oplysninger for personer, der er registreret i ind- og udrejsesystemet, VIS, ETIAS, Eurodac og ECRIS-TCN. Det bør være en del af den tekniske arkitektur for disse systemer og fungere som den fælles komponent mellem dem til lagring af og forespørgsel i identitetsoplysningerne, rejsedokumentoplysningerne og de biometriske oplysninger.

(27) Alle registreringer i CIR bør adskilles logisk ved automatisk at markere de enkelte registreringer med navnet på det underliggende system, som registreringen ligger i. Adgangskontrollen til CIR bør anvende disse markeringer til at bestemme, om der skal gives adgang til registreringen.

(28) Hvis en medlemsstats politimyndighed er ude af stand til at identificere en person på grund af fraværet af et rejsedokument eller et andet troværdigt dokument, der beviser vedkommendes identitet, eller hvis der hersker tvivl om rigtigheden af de identitetsoplysninger, personen opgiver, eller om rejsedokumentets ægthed eller dets indehavers identitet, eller hvis personen er ude af stand til eller nægter at samarbejde, bør denne politimyndighed kunne foretage en forespørgsel i CIR med henblik på at identificere personen. Med henblik herpå bør politimyndigheden registrere fingeraftryk ved hjælp af »live scan«-fingeraftrykteknikker, forudsat at proceduren blev indledt i den pågældende persons tilstedeværelse. Sådanne forespørgsler i CIR bør ikke tillades med henblik på identifikation af mindreårige under 12 år, medmindre det er i overensstemmelse med barnets tarv.

(29) Hvis en persons biometriske oplysninger ikke kan bruges, eller hvis en forespørgsel med disse oplysninger ikke lykkes, bør forespørgslen foretages med identitetsoplysninger for personen i kombination med rejsedokumentoplysninger. Hvis forespørgslen viser, at oplysninger om denne person er lagret i CIR, bør medlemsstatsmyndighederne have adgang til CIR for at konsultere denne persons identitetsoplysninger og rejsedokumentoplysninger, uden CIR giver nogen angivelse af, hvilket EU-informationssystem oplysningerne hører til.

(30) Medlemsstaterne bør vedtage nationale lovgivningsmæssige foranstaltninger for at udpege de myndigheder, der er kompetente til at foretage identitetskontrol ved hjælp af CIR, og fastsætte procedurer, betingelser og kriterier for sådan kontrol, der bør følge proportionalitetsprincippet. Navnlig bør beføjelserne for en medarbejder hos disse myndigheder til at indsamle biometriske oplysninger under en identitetskontrol af en person fastsættes i national ret.

(31) Denne forordning bør også indføre en ny mulighed for strømlinet adgang til oplysninger ud over de identitetsoplysninger eller rejsedokumentoplysninger, der findes i ind- og udrejsesystemet, VIS, ETIAS eller Eurodac, for de af medlemsstaterne udpegede myndigheder med ansvar for forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger, samt Europol. Sådanne oplysninger kan være nødvendige for at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger i en konkret sag, hvor der er rimelig grund til at antage, at en konsultation af dem vil bidrage til forebyggelsen, afsløringen eller efterforskningen af terrorhandlinger eller andre alvorlige strafbare handlinger, navnlig når der er mistanke om, at en person, der er mistænkt for, gerningsmand til eller offer for en terrorhandling eller anden alvorlig strafbar handling, er en person, hvis oplysninger er lagret i ind- og udrejsesystemet, VIS, ETIAS eller Eurodac.

(32) Fuld adgang til oplysninger indeholdt i EU-informationssystemerne, som er nødvendige med henblik på at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger, ud over adgang til identitetsoplysninger eller rejsedokumentoplysninger opbevaret i CIR, bør fortsat være omfattet af de gældende retlige instrumenter. De udpegede myndigheder med ansvar for forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger og Europol ved ikke på forhånd, hvilke af EU-informationssystemerne der indeholder oplysninger om de personer, de har brug for at forespørge om. Dette resulterer i forsinkelser og ineffektivitet. En slutbruger, som er autoriseret af den udpegede myndighed, bør derfor have lov til at se, i hvilke af disse EU-informationssystemer oplysningerne, der svarer til svaret på en forespørgsel, er registreret. Det berørte system vil dermed blive markeret efter den automatiske verifikation af, om der er et match i systemet (en såkaldt »match flag«-funktion).

(33) I denne sammenhæng bør et svar fra CIR ikke tolkes eller benyttes som begrundelse for at drage konklusioner om eller træffe foranstaltninger vedrørende en person, men bør kun anvendes med henblik på at indgive en anmodning om adgang til de underliggende EU-informationssystemer på de betingelser og efter de procedurer, der er fastsat i de respektive retlige instrumenter sådan adgang. Enhver sådan anmodning om adgang bør være underlagt denne forordnings kapitel VII og, alt efter hvad der er relevant, Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([5]), Europa-Parlamentets og Rådets direktiv (EU) 2016/680 ([6]) eller Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([7]).

(34) Som hovedregel bør de udpegede myndigheder eller Europol, når et »match flag« markerer, at oplysningerne er registreret i Eurodac, anmode om fuld adgang til mindst ét af de berørte EU-informationssystemer. Såfremt der undtagelsesvist ikke anmodes om en sådan fuld adgang, f.eks. fordi de udpegede myndigheder eller Europol allerede har indhentet oplysningerne på anden vis, eller fordi det ikke længere er tilladt at indhente oplysningerne i henhold til national ret, bør begrundelsen for ikke at anmode om adgang registreres.

(35) Logfilerne over forespørgsler i CIR bør vise formålet med forespørgslerne. Hvor en sådan forespørgsel blev udført ved hjælp af totrinstilgangen, bør logfilerne indeholde en henvisning til den nationale mappe for undersøgelsen eller sagen og derved angive, at forespørgslen blev foretaget med henblik på at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger.

(36) Udpegede myndigheders og Europols forespørgsel i CIR med henblik på at opnå et svar med »match flag«, der markerer, at oplysningerne er registreret i ind- og udrejsesystemet, VIS, ETIAS eller Eurodac, kræver automatiseret behandling af personoplysninger. Et »match flag« bør ikke vise personoplysninger om den pågældende person, men blot markere, at nogle af dennes oplysninger er lagret i et af systemerne. Den autoriserede slutbruger bør ikke træffe nogen negativ afgørelse vedrørende den berørte person alene på grundlag af den simple forekomst af et »match flag«. Slutbrugerens adgang til et »match flag« vil derfor udgøre et meget begrænset indgreb i retten til beskyttelse af personoplysninger om den berørte person, samtidig med at det vil give de udpegede myndigheder og Europol lov til at anmode om adgang til personoplysninger mere effektivt.

(37) MID bør oprettes for at støtte CIR's funktion og målene for ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN. For effektivt at kunne opfylde deres mål, kræver alle disse EU-informationssystemer en nøjagtig identifikation af de personer, hvis personoplysninger er lagret i dem.

(38) For bedre at opfylde EU-informationssystemernes mål bør de myndigheder, der anvender systemerne, være i stand til at foretage en tilstrækkeligt pålidelig verifikation af identiteten af de personer, hvis oplysninger er lagret i de forskellige systemer. De identitetsoplysninger eller rejsedokumentoplysninger, som er lagret i et givet

---

([5]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

([6]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89).

([7]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

individuelt system, kan være ukorrekte, ufuldstændige eller svigagtige, og der er i øjeblikket ingen mulighed for at afsløre ukorrekte, ufuldstændige eller svigagtige identitetsoplysninger eller rejsedokumentoplysninger ved at sammenligne med oplysninger, der er lagret i et andet system. For at afhjælpe denne situation er det nødvendigt at have et teknisk instrument på EU-plan, der gør det muligt nøjagtigt at identificere personer til disse formål.

(39) MID bør oprette og lagre links mellem oplysninger i de forskellige EU-informationssystemer med henblik på at påvise flere identiteter, både for at lette identitetskontrollen af bona fide-rejsende og bekæmpe identitetssvig. MID bør kun indeholde links mellem oplysninger om personer, der optræder i mere end ét EU-informationssystem. De sammenkædede oplysninger bør være strengt begrænset til de oplysninger, som er nødvendige for at verificere, at en person på berettiget eller uberettiget vis er registreret under forskellige identiteter i forskellige systemer, eller for at præcisere, at to personer med ensartede identitetsoplysninger måske ikke er den samme person. Databehandling gennem ESP og den fælles BMS for at forbinde de individuelle mapper på tværs af de forskellige systemer bør holdes på et absolut minimum og derfor begrænses til påvisning af flere identiteter på det tidspunkt, hvor nye oplysninger tilføjes i et af de systemer, der har oplysninger lagret i CIR, eller tilføjes i SIS. MID bør omfatte sikkerhedsforanstaltninger mod potentiel forskelsbehandling og ugunstige afgørelser vedrørende personer med flere lovlige identiteter.

(40) Denne forordning indeholder bestemmelser om nye databehandlingsaktiviteter til korrekt identifikation af de berørte personer. Dette udgør et indgreb i deres grundlæggende rettigheder, som er beskyttet af artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder. Eftersom en effektiv gennemførelse af EU-informationssystemerne afhænger af, at der foretages korrekt identifikation af de berørte personer, er et sådant indgreb begrundet i de samme mål, som hvert af disse systemer er blevet oprettet for, nemlig den effektive forvaltning af Unionens grænser, Unionens interne sikkerhed og den effektive gennemførelse af Unionens asyl- og visumpolitik.

(41) ESP og den fælles BMS bør sammenligne oplysninger om personer i CIR og SIS, når en national myndighed eller et EU-agentur opretter eller uploader nye registreringer. En sådan sammenligning bør automatiseres. CIR og SIS bør bruge den fælles BMS til at afsløre mulige links på grundlag af biometriske oplysninger. CIR og SIS bør bruge ESP til at afsløre mulige links på grundlag af alfanumeriske oplysninger. CIR og SIS bør være i stand til at identificere de samme eller ensartede oplysninger om en person, der er lagret i flere systemer. Hvor det er tilfældet, bør der oprettes et link, der angiver, at det er den samme person. CIR og SIS bør konfigureres således, at mindre translitterations- eller stavefejl opdages på en sådan måde, at det ikke skaber nogen uberettiget hindring for den berørte person.

(42) Den nationale myndighed eller det EU-agentur, der registrerede oplysningerne i det respektive EU-informationssystem, bør bekræfte eller ændre disse links. Denne nationale myndighed eller dette EU-agentur bør have adgang til de oplysninger, der er lagret i CIR eller SIS og i MID med henblik på manuel verifikation af forskellige identiteter.

(43) En manuel verifikation af forskellige identiteter bør sikres af den myndighed, der har oprettet eller ajourført de oplysninger, der udløste et match, som resulterede i et link til oplysninger, der er lagret i et andet EU-informationssystem. Den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, bør vurdere, om der er flere identiteter, der på berettiget eller uberettiget vis henviser til den samme person. En sådan vurdering bør så vidt muligt foretages i nærværelse af den berørte person og om nødvendigt ved at anmode om yderligere præciseringer eller oplysninger. Vurderingen bør udføres straks og i overensstemmelse med de retlige krav med hensyn til nøjagtigheden af oplysninger i henhold til EU-retten og national ret.

(44) Med hensyn til links, der er opnået via SIS, vedrørende indberetninger om personer, der begæres anholdt med henblik på overgivelse eller udlevering, om forsvundne eller sårbare personer, om personer, der eftersøges med henblik på at yde bistand i forbindelse med en retssag, eller om personer, der er genstand for diskret kontrol, undersøgelseskontrol eller målrettet kontrol, bør den myndighed, der er ansvarlig for den manuelle verifikation af

forskellige identiteter, være SIRENE-kontoret i den medlemsstat, der oprettede indberetningen. Disse kategorier af SIS-indberetninger er følsomme og bør ikke nødvendigvis deles med de myndigheder, der oprettede eller ajourførte oplysningerne, der er sammenkædet med dem, i et af de andre EU-informationssystemer. Oprettelsen af et link til SIS-oplysninger bør ikke berøre de tiltag, der skal træffes i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2018/1860 ([8]), (EU) 2018/1861 ([9]) og (EU) 2018/1862 ([10]).

(45) Oprettelsen af sådanne links kræver gennemsigtighed i forhold til de berørte personer. For at lette gennemførelsen af de nødvendige garantier i overensstemmelse med gældende EU-databeskyttelsesregler bør personer, for hvilke der er oprettet et rødt eller et hvidt link efter manuel verifikation af forskellige identiteter, informeres skriftligt, dog med forbehold af begrænsninger med henblik på at beskytte sikkerheden og den offentlige orden, forebygge kriminalitet og sikre, at nationale undersøgelser ikke bringes i fare. De pågældende personer bør modtage et enkelt identifikationsnummer, der sætter dem i stand til at identificere den myndighed, som de skal henvende sig til for at gøre deres rettigheder gældende.

(46) Hvor der oprettes et gult link, bør den myndighed, der er ansvarlig for den manuelle verifikationen af forskellige identiteter, have adgang til MID. Hvor der er et rødt link, bør medlemsstatsmyndigheder og EU-agenturer, der har adgang til mindst ét EU-informationssystem, der indgår i CIR eller SIS, have adgang til MID. Et rødt link markerer, at en person uberettiget bruger forskellige identiteter, eller at en person bruger en anden persons identitet.

(47) Hvor der findes et hvidt eller grønt link mellem oplysninger fra to EU-informationssystemer, bør medlemsstats-myndigheder og EU-agenturer have adgang til MID, hvor den berørte myndighed eller det berørte agentur har adgang til begge informationssystemer. En sådan adgang bør udelukkende gives med det formål at gøre det muligt for denne myndighed eller dette agentur at afsløre potentielle tilfælde, hvor oplysninger er ukorrekt sammenkædet eller behandlet i MID, CIR og SIS i strid med denne forordning, og træffes tiltag til at rette op på situationen og ajourføre eller slette linket.

(48) Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) bør indføre automatiserede kontrolmekanismer for datakvalitet og fælles datakvalitetsindikatorer. eu-LISA bør være ansvarlig for at udvikle en central overvågningskapacitet for datakvalitet og for at udarbejde regelmæssige dataanalyserapporter for at forbedre kontrollen med medlemsstaternes gennemførelse af EU-informationssystemer. De fælles datakvalitetsindikatorer bør omfatte minimumskvalitetsstandarder for lagring af oplysninger i EU-informationssystemerne eller interoperabilitetskomponenterne. Målet med sådanne datakvalitetsstandarder bør være, at EU-informationssystemerne og interoperabilitetskomponenterne automatisk kan finde tilsyneladende forkerte eller inkonsekvente registreringer af oplysninger, så den medlemsstat, hvorfra oplysningerne kommer, kan verificere oplysningerne og træffe eventuelle nødvendige afhjælpende tiltag.

(49) Kommissionen bør evaluere eu-LISA's kvalitetsrapporter og i passende omfang, hvor det er hensigtsmæssigt, fremsætte henstillinger til medlemsstaterne. Medlemsstaterne bør have ansvaret for at udarbejde en handlingsplan, der beskriver tiltag for at rette op på eventuelle mangler i forhold til datakvalitet, og bør løbende aflægge rapport om dens fremskridt.

(50) Det universelle meddelelsesformat (UMF) bør være standard for struktureret, grænseoverskridende informations-udveksling mellem informationssystemer, myndigheder og organisationer på området for retlige og indre anliggender. UMF bør fastsætte et fælles ordforråd og logiske strukturer til almindeligt udvekslede oplysninger med det formål at lette interoperabiliteten ved at muliggøre, at indholdet af udvekslede oplysninger kan fastsættes og læses på en konsekvent og semantisk ækvivalent måde.

(51) Det kan overvejes at gennemføre UMF-standarden i VIS, SIS og i andre eksisterende eller nye modeller for grænseoverskridende informationsudveksling og informationssystemer på området for retlige og indre anliggender, som er udviklet af medlemsstaterne.

([8]) Europa-Parlamentets og Rådets forordning (EU) 2018/1860 af 28. november 2018 om brug af Schengeninformationssystemet i forbindelse med tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold (EUT L 312 af 7.12.2018, s. 1).

([9]) Europa-Parlamentets og Rådets forordning (EU) 2018/1861 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området ind- og udrejsekontrol, om ændring af konventionen om gennemførelse af Schengenaftalen og om ændring og ophævelse af forordning (EF) nr. 1987/2006 (EUT L 312 af 7.12.2018, s. 14).

([10]) Europa-Parlamentets og Rådets forordning (EU) 2018/1862 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området politisamarbejde og strafferetligt samarbejde, om ændring og ophævelse af Rådets afgørelse 2007/533/RIA og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1986/2006 og Kommissionens afgørelse 2010/261/EU (EUT L 312 af 7.12.2018, s. 56).

(52) Der bør oprettes et centralt register for rapportering og statistik (CRRS), der skal generere statistiske oplysninger og analytisk rapportering på tværs af systemerne til politiske, operationelle og datakvalitetsmæssige formål i overensstemmelse med de gældende retlige instrumenter. eu-LISA bør oprette, gennemføre og hoste CRRS på sine tekniske anlæg. Det bør indeholde anonymiserede statistiske oplysninger fra EU-informationssystemerne, CIR, MID og den fælles BMS. De oplysninger, der er indeholdt i CRRS, bør ikke gøre det muligt at identificere enkeltpersoner. eu-LISA bør anonymisere oplysningerne på automatiseret vis og registrere sådanne anonymiserede oplysninger i CRRS. Processen med at anonymisere oplysninger bør automatiseres, og eu-LISA's personale bør ikke gives direkte adgang til personoplysninger, som er lagret i EU-informationssystemerne eller i interoperabilitetskomponenterne.

(53) Forordning (EU) 2016/679 finder anvendelse på de nationale myndigheders behandling af personoplysninger med henblik på interoperabilitet i henhold til nærværende forordning, medmindre en sådan behandling foretages af de udpegede myndigheder eller centrale adgangspunkter i medlemsstaterne med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger.

(54) Hvor medlemsstaternes behandling af personoplysninger med henblik på interoperabilitet i henhold til denne forordning foretages af de kompetente myndigheder med det formål at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger, finder direktiv (EU) 2016/680 anvendelse.

(55) Forordning (EU) 2016/679, (EU) 2018/1725 eller, hvor det er relevant, direktiv (EU) 2016/680 finder anvendelse på enhver overførsel af personoplysninger til tredjelande eller internationale organisationer, der finder sted i henhold til nærværende forordning. Uden at det berører grundene til overførsel i henhold til kapitel V i forordning (EU) 2016/679 eller, hvor det er relevant, direktiv (EU) 2016/680, bør en afgørelse truffet af en domstol eller af en administrativ myndighed i et tredjeland, der kræver, at en dataansvarlig eller en databehandler overfører eller videregiver personoplysninger, kun anerkendes eller kunne håndhæves på nogen måde, hvis den bygger på en gældende international aftale mellem det anmodende tredjeland og Unionen eller en medlemsstat.

(56) De særlige bestemmelser om databeskyttelse i forordning (EU) 2018/1862 og Europa-Parlamentets og Rådets forordning (EU) 2019/816 ([11]) finder anvendelse på behandlingen af personoplysninger i de systemer, der reguleres ved nævnte forordninger.

(57) Forordning (EU) 2018/1725 finder anvendelse på eu-LISA's og andre EU-institutioners og -organers behandling af personoplysninger, når de udfører deres opgaver i henhold til nærværende forordning, uden at det berører forordning (EU) 2016/794, som finder anvendelse på behandlingen af personoplysninger i Europol.

(58) De i forordning (EU) 2016/679 eller direktiv (EU) 2016/680 omhandlede tilsynsmyndigheder bør overvåge lovligheden af medlemsstaternes behandling af personoplysninger. Den Europæiske Tilsynsførende for Databeskyttelse bør overvåge EU-institutionernes og -organernes aktiviteter i forbindelse med behandlingen af personoplysninger. Den Europæiske Tilsynsførende for Databeskyttelse og tilsynsmyndighederne bør samarbejde om at overvåge behandlingen af personoplysninger i interoperabilitetskomponenterne. For at sætte Den Europæiske Tilsynsførende for Databeskyttelse i stand til at udføre sine opgaver i henhold til nærværende forordning kræves der tilstrækkelige ressourcer, herunder af både menneskelig og finansiel karakter.

(59) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 28, stk. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 ([12]), og afgav en udtalelse den 16. april 2018 ([13]).

(60) Artikel 29-Gruppen vedrørende Databeskyttelse afgav en udtalelse den 11. april 2018.

(61) Både medlemsstaterne og eu-LISA bør opretholde sikkerhedsplaner for at lette gennemførelsen af sikkerhedsforpligtelser og bør samarbejde indbyrdes om at tage hånd om sikkerhedsspørgsmål. eu-LISA bør også sikre, at den seneste teknologiske udvikling udnyttes kontinuerligt for at sikre dataintegritet for så vidt angår udvikling, udformning og forvaltning af interoperabilitetskomponenterne. eu-LISA's forpligtelser i denne henseende bør omfatte vedtagelse af de nødvendige foranstaltninger til at forhindre, at personer uden bemyndigelse, såsom

---

([11]) Europa-Parlamentets og Rådets forordning (EU) 2019/816 af 17. april 2019 om oprettelse af et centralt system til bestemmelse af, hvilke medlemsstater der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer (ECRIS-TCN) for at supplere det europæiske informationssystem vedrørende strafferegistre, og om ændring af forordning (EU) 2018/1726 Se side 1 i denne EUT.

([12]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

([13]) EUT C 233 af 4.7.2018, s. 12.

eksterne tjenesteyderes personale, får adgang til personoplysninger, der behandles via interoperabilitetskomponenterne. Når medlemsstaterne og eu-LISA tildeler kontrakter om levering af tjenesteydelser, bør de overveje alle foranstaltninger, der er nødvendig for at sikre overholdelsen af love eller bestemmelser vedrørende beskyttelse af personoplysninger og enkeltpersoners privatliv og for at beskytte væsentlige sikkerhedsinteresser i henhold til Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 ([14]) og gældende internationale konventioner. eu-LISA bør anvende principperne om privatlivsbeskyttelse gennem design og som standard under udviklingen af interoperabilitetskomponenterne.

(62) For at understøtte både statistik og rapportering er det nødvendigt at give adgang til bemyndigede medarbejdere i de kompetente myndigheder, EU-institutioner og -agenturer, der er omhandlet i denne forordning, til at benytte visse oplysninger vedrørende visse interoperabilitetskomponenter uden at gøre identifikation af enkeltpersoner mulig.

(63) For at give medlemsstaternes myndigheder og EU-agenturerne mulighed for at tilpasse sig de nye krav om brug af ESP er det nødvendigt at fastsætte en overgangsperiode. Ligeledes bør der med henblik på at give MID mulighed for at fungere sammenhængende og optimalt etableres overgangsforanstaltninger, når driften deraf indledes.

(64) Målet for denne forordning, nemlig fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union (TEU). I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål.

(65) Det resterende beløb på budgettet øremærket til intelligente grænser i Europa-Parlamentets og Rådets forordning (EU) nr. 515/2014 ([15]) bør omfordeles til nærværende forordning i medfør af artikel 5, stk. 5, litra b), i forordning (EU) nr. 515/2014 for at dække omkostningerne ved udvikling af interoperabilitetskomponenterne.

(66) For at supplere visse detaljerede tekniske aspekter af denne forordning bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) for så vidt angår:

— forlængelse af overgangsperioden for anvendelsen af ESP

— forlængelse af overgangsperioden for påvisning af flere identiteter, der udføres af den centrale ETIAS-enhed

— procedurerne for bestemmelse af de tilfælde, hvor identitetsoplysninger kan betragtes som de samme eller ensartede

— reglerne for driften af CRRS, inklusive særlige sikkerhedsforanstaltninger i forbindelse med behandling af personoplysninger og sikkerhedsreglerne for registeret, og

— detaljerede regler for driften af webportalen.

Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning ([16]). For at sikre lige deltagelse i udarbejdelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(67) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser til at fastlægge de datoer, fra hvilke ESP, fælles BMS, CIF, MID og CRRS skal sættes i drift.

([14]) Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget, om ændring af forordning (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 og afgørelse nr. 541/2014/EU og om ophævelse af forordning (EU, Euratom) nr. 966/2012 (EUT L 193 af 30.7.2018, s. 1).

([15]) Europa-Parlamentets og Rådets forordning (EU) nr. 515/2014 af 16. april 2014 om oprettelse af et instrument for finansiel støtte til forvaltning af de ydre grænser og den fælles visumpolitik som en del af Fonden for Intern Sikkerhed og om ophævelse af beslutning nr. 574/2007/EF (EUT L 150 af 20.5.2014, s. 143).

([16]) EUT L 123 af 12.5.2016, s. 1.

(68) Kommission bør også tillægges gennemførelsesbeføjelser vedrørende vedtagelsen af nærmere regler om: de tekniske detaljer for ESP-brugerprofiler; specifikationerne for den tekniske løsning, der vil gøre det muligt at forespørge i EU-informationssystemerne, Europol-oplysninger og INTERPOL-databaserne ved hjælp af ESP, samt formatet af ESP-svarene; de tekniske regler for oprettelse af links i MID mellem oplysninger fra forskellige EU-informationssystemer; indholdet og udseendet af formularen for underretning af den registrerede, når der oprettes et rødt link; kravene til og overvågning af den fælles BMS' resultater; automatiserede datakvalitetskontrolmekanismer, -procedurer og -indikatorer; udviklingen af UMF-standarden; den samarbejdsprocedure, der skal bruges i tilfælde af en sikkerhedshændelse; og specifikationerne for den tekniske løsning for medlemsstaternes forvaltning af brugeranmodninger om adgang. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ([17]).

(69) Eftersom interoperabilitetskomponenter vil omfatte behandlingen af store mængder følsomme personoplysninger, er det vigtigt, at personer, hvis personoplysninger behandles gennem disse komponenter, effektivt kan udøve deres rettigheder som registrerede som krævet i henhold til forordning (EU) 2016/679, direktiv (EU) 2016/680 og forordning (EU) 2018/1725. De registrerede bør have adgang til en webportal, der letter udøvelsen af deres ret til indsigt i samt berigtigelse, sletning og begrænsning af behandling af deres personoplysninger. eu-LISA bør oprette og forvalte en sådan webportal.

(70) Et af kerneprincipperne for databeskyttelse er dataminimering: I henhold til artikel 5, stk. 1, litra c), i forordning (EU) 2016/679 skal behandling af personoplysninger være tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles. Interoperabilitetskomponenterne bør derfor ikke omfatte lagring af nye personoplysninger med undtagelse af de links, som vil blive lagret i MID, og som udgør det nødvendige minimum for at opfylde formålet med nærværende forordning.

(71) Denne forordning bør indeholde klare bestemmelser om erstatningsansvar og retten til erstatning for ulovlig behandling af personoplysninger og for enhver anden handling, der er i strid med denne forordning. Sådanne bestemmelser bør ikke berøre retten til erstatning fra den dataansvarlige eller databehandleren, samt deres erstatningsansvar, i henhold til forordning (EU) 2016/679, direktiv (EU) 2016/680 og forordning (EU) 2018/1725. eu-LISA bør være ansvarlig for enhver skade, det forvolder i dets egenskab af databehandler, hvor det ikke har opfyldt de forpligtelser, som det udtrykkeligt er pålagt i henhold til nærværende forordning, eller hvor det har undladt at følge eller har handlet i strid med lovlige instrukser fra den medlemsstat, som er dataansvarlig.

(72) Denne forordning berører ikke anvendelsen af Europa-Parlamentets og Rådets direktiv 2004/38/EF ([18]).

(73) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til TEU og til TEUF, deltager Danmark ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Danmark. Inden seks måneder efter, at Rådet har truffet foranstaltning om denne forordning, der for så vidt dens bestemmelser vedrører SIS som reguleret af forordning (EU) 2018/1862 bygger på Schengenreglerne, træffer Danmark afgørelse om, hvorvidt det vil gennemføre denne forordning i sin nationale lovgivning, jf. artikel 4 i protokollen.

(74) For så vidt som nærværende forordnings bestemmelser vedrører SIS som reguleret ved forordning (EU) 2018/1862, deltager Det Forenede Kongerige i nærværende forordning i overensstemmelse med artikel 5, stk. 1, i protokol nr. 19 om Schengenreglerne som integreret i Den Europæiske Union, der er knyttet som bilag til TEU og til TEUF, og artikel 8, stk. 2, i Rådets afgørelse 2000/365/EF ([19]). For så vidt som nærværende forordnings bestemmelser vedrører Eurodac og ECRIS-TCN, jf. artikel 3 i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til TEU og til TEUF, har Det Forenede Kongerige endvidere ved skrivelse af 18. maj 2018 meddelt, at det ønsker at deltage i vedtagelsen og anvendelsen af nærværende forordning.

([17]) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

([18]) Europa-Parlamentets og Rådets direktiv 2004/38/EF af 29. april 2004 om unionsborgeres og deres familiemedlemmers ret til at færdes og opholde sig frit på medlemsstaternes område, om ændring af forordning (EØF) nr. 1612/68 og om ophævelse af direktiv 64/221/EØF, 68/360/EØF, 72/194/EØF, 73/148/EØF, 75/34/EØF, 75/35/EØF, 90/364/EØF, 90/365/EØF og 93/96/EØF (EUT L 158 af 30.4.2004, s. 77).

([19]) Rådets afgørelse 2000/365/EF af 29. maj 2000 om anmodningen fra Det Forenede Kongerige Storbritannien og Nordirland om at deltage i visse af bestemmelserne i Schengenreglerne (EFT L 131 af 1.6.2000, s. 43).

(75) For så vidt som nærværende forordnings bestemmelser vedrører SIS som reguleret ved forordning (EU) 2018/1862, kunne Irland i princippet deltage i nærværende forordning i overensstemmelse med artikel 5, stk. 1, i protokol nr. 19 om Schengenreglerne som integreret i Den Europæiske Union, der er knyttet som bilag til TEU og til TEUF, og artikel 6, stk. 2, i Rådets afgørelse 2002/192/EF ([20]). For så vidt som nærværende forordnings bestemmelser vedrører Eurodac og ECRIS-TCN, jf. artikel 1 og 2 i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til TEU og til TEUF, og uden at det berører nævnte protokols artikel 4, deltager Irland endvidere ikke i vedtagelsen af nærværende forordning, som ikke er bindende for og ikke finder anvendelse i Irland. Eftersom det under disse omstændigheder ikke er muligt at sikre, at nærværende forordning finder anvendelse i Irland i alle enkeltheder som fastsat i artikel 288 i TEUF, deltager Irland ikke i vedtagelsen af nærværende forordning, som ikke er bindende for og ikke finder anvendelse i Irland, uden at dette berører Irlands rettigheder i medfør af protokol nr. 19 og 21.

(76) For så vidt angår Island og Norge udgør denne forordning, for så vidt som den vedrører SIS som reguleret af forordning (EU) 2018/1862, en udvikling af de bestemmelser i Schengenreglerne, jf. aftalen indgået mellem Rådet for Den Europæiske Union og Republikken Island og Kongeriget Norge om disse to staters associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne ([21]), der henhører under det område, som er nævnt i artikel 1, litra G, i Rådets afgørelse 1999/437/EF ([22]).

(77) For så vidt angår Schweiz udgør denne forordning, for så vidt som den vedrører SIS som reguleret af forordning (EU) 2018/1862, en udvikling af de bestemmelser i Schengenreglerne, jf. aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne ([23]), der henhører under det område, som er nævnt i artikel 1, litra G, i afgørelse 1999/437/EF sammenholdt med artikel 3 i Rådets afgørelse 2008/149/RIA ([24]).

(78) For så vidt angår Liechtenstein udgør denne forordning, for så vidt som den vedrører SIS som reguleret af forordning (EU) 2018/1862, en udvikling af de bestemmelser i Schengenreglerne, jf. protokollen mellem Den Europæiske Union, Det Europæiske Fællesskab, Det Schweiziske Forbund og Fyrstendømmet Liechtenstein om Fyrstendømmet Liechtensteins tiltrædelse af aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne ([25]), der henhører under det område, der er nævnt i artikel 1, litra G, i afgørelse 1999/437/EF, sammenholdt med artikel 3 i Rådets afgørelse 2011/350/EU ([26]).

(79) Denne forordning respekterer de grundlæggende rettigheder og overholder de principper, som navnlig er anerkendt i Den Europæiske Unions charter om grundlæggende rettigheder, og bør anvendes i overensstemmelse med disse rettigheder og principper.

(80) For at denne forordning kan passe ind i den eksisterende retlige ramme, bør Europa-Parlamentets og Rådets forordning (EU) 2018/1726 ([27]), (EU) 2018/1862 og (EU) 2019/816 ændres i overensstemmelse hermed —

([20]) Rådets afgørelse 2002/192/EF af 28. februar 2002 om anmodningen fra Irland om at deltage i visse af bestemmelserne i Schengen-reglerne (EFT L 64 af 7.3.2002, s. 20).

([21]) EFT L 176 af 10.7.1999, s. 36.

([22]) Rådets afgørelse 1999/437/EF af 17. maj 1999 om visse gennemførelsesbestemmelser til den aftale, som Rådet for Den Europæiske Union har indgået med Republikken Island og Kongeriget Norge om disse to staters associering i gennemførelsen, anvendelsen og den videre udvikling af Schengen-reglerne (EFT L 176 af 10.7.1999, s. 31).

([23]) EUT L 53 af 27.2.2008, s. 52.

([24]) Rådets afgørelse 2008/149/RIA af 28. januar 2008 om indgåelse, på Den Europæiske Unions vegne, af aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne (EUT L 53 af 27.2.2008, s. 50).

([25]) EUT L 160 af 18.6.2011, s. 21.

([26]) Rådets afgørelse 2011/350/EU af 7. marts 2011 om indgåelse, på Den Europæiske Unions vegne, af protokollen mellem Den Europæiske Union, Det Europæiske Fællesskab, Det Schweiziske Forbund og Fyrstendømmet Liechtenstein om Fyrstendømmet Liechtensteins tiltrædelse af aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne, navnlig for så vidt angår afskaffelsen af kontrollen ved de indre grænser og personbevægelser (EUT L 160 af 18.6.2011, s. 19).

([27]) Europa-Parlamentets og Rådets forordning (EU) 2018/1726 af 14. november 2018 om Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) og om ændring af forordning (EF) nr. 1987/2006 og Rådets afgørelse 2007/533/RIA og om ophævelse af forordning (EU) nr. 1077/2011 (EUT L 295 af 21.11.2018, s. 99).

VEDTAGET DENNE FORORDNING:

KAPITEL I

Almindelige bestemmelser

Artikel 1

Genstand

1. Denne forordning fastsætter sammen med Europa-Parlamentets og Rådets forordning (EU) 2019/817 ([28]) en ramme, der skal sikre interoperabilitet mellem ind-og udrejsesystemet, visuminformationssystemet (VIS), EU-systemet vedrørende rejseinformation og rejsetilladelse (ETIAS), Eurodac, Schengeninformationssystemet (SIS) og det europæiske informationssystem til udveksling af oplysninger fra strafferegistre vedrørende tredjelandsstatsborgere (ECRIS-TCN).

2. Rammen omfatter følgende interoperabilitetskomponenter:

a) en europæisk søgeportal (ESP)

b) en fælles biometrisk matchtjeneste (fælles BMS)

c) et fælles identitetsregister(CIR)

d) en multiidentitetsdetektor (MID).

3. Denne forordning fastsætter også bestemmelser om datakvalitetskrav, om et universelt meddelelsesformat (UMF), om et centralt register for rapportering og statistik (CRRS) og om ansvarsområderne for medlemsstaterne og Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) med hensyn til udformningen, udviklingen og driften af interoperabilitetskomponenter.

4. Denne forordning tilpasser også procedurerne og betingelserne for adgangen for de udpegede myndigheder og Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) til ind- og udrejsesystemet, VIS, ETIAS og Eurodac med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger.

5. Denne forordning fastsætter også en ramme for verifikation af personers identitet og for identifikation af personer.

Artikel 2

Mål

1. Ved at sikre interoperabilitet har denne forordning følgende mål:

a) at forbedre effektiviteten og formålstjenligheden af ind- og udrejsekontrollen ved de ydre grænser

b) at bidrage til forebyggelsen og bekæmpelsen af ulovlig indvandring

c) at bidrage til et højt sikkerhedsniveau inden for området med frihed, sikkerhed og retfærdighed, herunder at opretholde den offentlige sikkerhed og den offentlige orden samt beskytte sikkerheden på medlemsstaternes område

d) at forbedre gennemførelsen af den fælles visumpolitik

e) at bistå ved gennemgangen af ansøgninger om international beskyttelse

f) at bidrage til forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger

g) at lette identifikationen af ukendte personer, der er ude af stand til at legitimere sig, eller uidentificerede menneskelige rester i tilfælde af en naturkatastrofe, en ulykke eller et terrorangreb.

2. De i stk. 1 omhandlede mål skal nås ved at:

a) sikre korrekt identifikation af personer

b) bidrage til bekæmpelse af identitetssvig

([28]) Europa-Parlamentets og Rådets forordning (EU) 2019/817 af 20. maj 2019 om fastsættelse af en ramme for interoperabiliteten mellem EU-informationssystemer vedrørende grænser og visum og om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 og (EU) 2018/1861, Rådets beslutning 2004/512/EF og Rådets afgørelse 2008/633/RIA (se side 27 i denne EUT).

c) forbedre datakvalitet og harmonisere kvalitetskravene til oplysninger, der lagres i EU-informationssystemerne, under overholdelse af databehandlingskravene i de retlige instrumenter for de enkelte systemer, databeskyttelsesstandarderne og -principperne

d) lette og understøtte medlemsstaternes tekniske og operationelle gennemførelse af EU-informationssystemer

e) styrke og forenkle de betingelser for datasikkerhed og databeskyttelse, der styrer de respektive EU-informationssystemer, og gøre dem mere ensartede uden at påvirke den særlige beskyttelse og de sikkerhedsmekanismer, der er gældende for visse kategorier af oplysninger

f) effektivisere betingelserne for udpegede myndigheders adgang til ind- og udrejsesystemet, VIS, ETIAS og Eurodac og samtidig sikre nødvendige og forholdsmæssigt afpassede betingelser for denne adgang

g) støtte formålene med ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN.

Artikel 3

Anvendelsesområde

1. Denne forordning gælder for Eurodac, SIS og ECRIS-TCN.

2. Denne forordning gælder også for Europoloplysningerne, i det omfang at det gøres muligt at forespørge i dem samtidigt med de i stk. 1 omhandlede EU-informationssystemer.

3. Denne forordning gælder for personer, hvis personoplysninger kan behandles i de i stk. 1 omhandlede EU-informationssystemer, og de i stk. 2 omhandlede Europoloplysninger.

Artikel 4

Definitioner

I denne forordning forstås ved:

1) »ydre grænser«: ydre grænser som defineret i artikel 2, nr. 2), i forordning (EU) 2016/399

2) »ind- og udrejsekontrol«: ind- og udrejsekontrol som defineret i artikel 2, nr. 11), i Europa-Parlamentets og Rådets forordning (EU) 2016/399 ([29])

3) »grænsemyndighed«: den grænsevagt, der i overensstemmelse med national ret er udpeget til at foretage ind- og udrejsekontrol

4) »tilsynsmyndigheder«: den tilsynsmyndighed, der er omhandlet i artikel 51, stk. 1, i forordning (EU) 2016/679, og den tilsynsmyndighed, der er omhandlet i artikel 41, stk. 1, i direktiv (EU) 2016/680

5) »verifikation«: sammenligning af sæt af oplysninger for at kontrollere, om en påstået identitet er ægte (kontrol ved sammenligning af to datasæt oplysninger)

6) »identifikation«: fastlæggelse af en persons identitet via en databasesøgning på grundlag af flere sæt oplysninger (kontrol ved sammenligning af mange sæt oplysninger)

7) »alfanumeriske oplysninger«: oplysninger, der er angivet med bogstaver, tal, specialtegn, mellemrum og skilletegn

8) »identitetsoplysninger«: de oplysninger, som er omhandlet i artikel 27, stk. 3, litra a)-e)

9) »fingeraftryksoplysninger«: fingeraftryksbilleder og latente fingeraftryksbilleder, som på grund af deres unikke karakter og referencepunkterne i dem gør det muligt at foretage præcise og endegyldige sammenligninger vedrørende en persons identitet

([29]) Europa-Parlamentets og Rådets forordning (EU) 2016/399 af 9. marts 2016 om en EU-kodeks for personers grænsepassage (Schengengrænsekodeks) (EUT L 77 af 23.3.2016, s. 1).

10) »ansigtsbillede«: digitale billeder af ansigtet

11) »biometriske oplysninger«: fingeraftryksoplysninger eller ansigtsbilleder eller begge

12) »biometrisk skabelon«: en matematisk gengivelse opnået ved at udlede træk fra biometriske oplysninger begrænset til de karakteristika, som er nødvendige for at foretage identifikationer og verifikationer

13) »rejsedokument«: et pas eller et andet tilsvarende dokument, som giver indehaveren ret til at passere de ydre grænser, og som kan forsynes med visum

14) »rejsedokumentoplysninger«: type, nummer og udstedelsesland for rejsedokumentet, udløbsdato for rejsedokumentets gyldighed og koden på tre bogstaver for det land, der har udstedt rejsedokumentet

15) »EU-informationssystemer«: ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN

16) »Europoloplysningerne«: personoplysninger, der behandles af Europol til de formål, der er omhandlet i artikel 18, stk. 2, litra a), b) og c), i forordning (EU) 2016/794

17) »INTERPOL-databaserne«: INTERPOL's database over stjålne og bortkomne rejsedokumenter (SLTD-databasen) og INTERPOL's database over rejsedokumenter med tilknyttede notifikationer (TDAWN-databasen)

18) »match«: sammenfald som resultat af en automatiseret sammenligning mellem personoplysninger, der er registreret eller er ved at blive registreret i et informationssystem eller en database

19) »politimyndighed«: den kompetente myndighed som defineret i artikel 3, nr. 7), i direktiv (EU) 2016/680

20) »udpegede myndigheder«: myndigheder udpeget af medlemsstaterne som defineret i artikel 3, stk. 1, nr. 26), i Europa-Parlamentets og Rådets forordning (EU) 2017/2226 ([30]), artikel 2, stk. 1, litra e), i Rådets afgørelse 2008/633/RIA ([31]) og artikel 3, stk. 1, nr. 21), i Europa-Parlamentets og Rådets forordning (EU) 2018/1240 ([32])

21) »terrorhandling«: en lovovertrædelse i henhold til national ret, som svarer til eller er ligestillet med en af de lovovertrædelser, der er omhandlet i Europa-Parlamentets og Rådets direktiv (EU) 2017/541 ([33])

22) »alvorlig strafbar handling«: en lovovertrædelse, som svarer til eller er ligestillet med en af de lovovertrædelser, der er omhandlet i artikel 2, stk. 2, i Rådets rammeafgørelse 2002/584/RIA ([34]), hvis den i henhold til national ret kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år

23) »ind- og udrejsesystemet«: ind- og udrejsesystemet oprettet ved forordning (EU) 2017/2226

24) »visuminformationssystemet« eller (»VIS«): visuminformationssystemet oprettet ved Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008 ([35])

25) »europæisk system vedrørende rejseoplysninger og rejsetilladelser« eller »ETIAS«: det europæiske system for rejseoplysninger og rejsetilladelser oprettet ved forordning (EU) 2018/1240

---

(30) Europa-Parlamentets og Rådets forordning (EU) 2017/2226 af 30. november 2017 om oprettelse af et ind- og udrejsesystem til registrering af ind- og udrejseoplysninger og oplysninger om nægtelse af indrejse vedrørende tredjelandsstatsborgere, der passerer medlemsstaternes ydre grænser, om fastlæggelse af betingelserne for adgang til ind- og udrejsesystemet til retshåndhævelsesformål og om ændring af konventionen om gennemførelse af Schengenaftalen og forordning (EF) nr. 767/2008 og (EU) nr. 1077/2011 (EUT L 327 af 9.12.2017, s. 20).

(31) Rådets afgørelse 2008/633/RIA af 23. juni 2008 om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (EUT L 218 af 13.8.2008, s. 129).

(32) Europa-Parlamentets og Rådets forordning (EU) 2018/1240 af 12. september 2018 om oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) og om ændring af forordning (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399 (EU) 2016/1624 og (EU) 2017/2226 (EUT L 236 af 19.9.2018, s. 1).

(33) Europa-Parlamentets og Rådets direktiv (EU) 2017/541 af 15. marts 2017 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA (EUT L 88 af 31.3.2017, s. 6).

(34) Rådets rammeafgørelse 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurerne for overgivelse mellem medlemsstaterne (EFT L 190 af 18.7.2002, s. 1).

(35) Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008 af 9. juli 2008 om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (VIS-forordningen) (EUT L 218 af 13.8.2008, s. 60).

26) »Eurodac«: Eurodac oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 ([36])

27) »Schengeninformationssystemet« eller »SIS«: Schengeninformationssystemet oprettet ved forordning (EU) 2018/1860, (EU) 2018/1861 og (EU) 2018/1862

28) »ECRIS-TCN«: det centraliserede system til indkredsning af medlemsstater, der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer, oprettet ved forordning (EU) 2019/816.

Artikel 5

Ikkeforskelsbehandling og grundlæggende rettigheder

Behandlingen af personoplysninger med henblik på denne forordning må ikke medføre forskelsbehandling af personer af nogen grunde, såsom køn, race, hudfarve, etnisk eller social oprindelse, genetiske anlæg, sprog, religion eller tro, politiske eller andre anskuelser, tilhørsforhold til et nationalt mindretal, ejendomsforhold, fødsel, handicap, alder eller seksuel orientering. Den skal fuldt ud respektere menneskelig værdighed og integritet og de grundlæggende rettigheder, herunder retten til respekt for privatliv og beskyttelse af personoplysninger. Der skal tages særligt hensyn til børn, ældre, personer med handicap og personer, der har behov for international beskyttelse. Hensynet til barnets tarv kommer i første række.

KAPITEL II

Europæisk søgeportal

Artikel 6

Europæisk søgeportal

1. Der oprettes en europæisk søgeportal (ESP) med henblik på at lette hurtig, problemfri, effektiv, systematisk og kontrolleret adgang for medlemsstatsmyndigheder og EU-agenturer til EU-informationssystemer, til Europoloplysningerne og til INTERPOL-databaserne i forbindelse med udførelsen af deres opgaver og i overensstemmelse med deres adgangsret og målene for og formålene med ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN.

2. ESP består af:

a) en central infrastruktur, herunder en søgeportal, der muliggør samtidige forespørgsler i ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN samt Europoloplysningerne og INTERPOL-databaserne

b) en sikker kommunikationskanal mellem ESP og de medlemsstater og EU-agenturer, der har ret til at bruge ESP

c) en sikker kommunikationsinfrastruktur mellem ESP og ind- og udrejsesystemet, VIS, ETIAS, Eurodac, det centrale SIS, ECRIS-TCN, Europoloplysningerne og INTERPOL-databaserne samt mellem ESP og de centrale infrastrukturer i CIR og MID.

3. eu-LISA udvikler og står for den tekniske forvaltning af ESP.

Artikel 7

Brug af den europæiske søgeportal

1. Brugen af ESP er forbeholdt de medlemsstatsmyndigheder og EU-agenturer, der har adgang til mindst ét af EU-informationssystemerne i overensstemmelse med de retlige instrumenter, der regulerer disse EU-informationssystemer, til CIR og MID i overensstemmelse med denne forordning, til Europol-oplysningerne i overensstemmelse med forordning (EU) 2016/794 eller til INTERPOL-databaserne i overensstemmelse med den EU-ret eller nationale ret, der regulerer sådan adgang.

Disse medlemsstatsmyndigheder og EU-agenturer må kun anvende ESP og de derigennem tilvejebragte oplysninger til de mål og formål, der er fastsat i de retlige instrumenter for disse EU-informationssystemer, i forordning (EU) 2016/794 og i nærværende forordning.

([36]) Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 af 26. juni 2013 om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet i en af medlemsstaterne af en tredjelandsstatsborger eller en statsløs og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse og om ændring af forordning (EU) nr. 1077/2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store it-systemer inden for området med frihed, sikkerhed og retfærdighed (EUT L 180 af 29.6.2013, s. 1).

2. De i stk. 1 omhandlede medlemsstatsmyndigheder og EU-agenturer bruger ESP til at søge efter oplysninger om personer eller deres rejsedokumenter i de centrale systemer i Eurodac og ECRIS-TCN i overensstemmelse med deres adgangsret som omhandlet i de retlige instrumenter, der regulerer disse EU-informationssystemer, og i national ret. De bruger også ESP til at foretage forespørgsler i CIR i overensstemmelse med deres adgangsret i henhold til denne forordning til de i artikel 20, 21 og 22 omhandlede formål.

3. De i stk. 1 omhandlede medlemsstatsmyndigheder kan bruge ESP til at søge efter oplysninger om personer eller deres rejsedokumenter i det i forordning (EU) 2018/1860 og (EU) 2018/1861 omhandlede centrale SIS.

4. Hvor det er foreskrevet EU-retten, bruger de i stk. 1 omhandlede EU-agenturer ESP til at søge efter oplysninger om personer eller deres rejsedokumenter i det centrale SIS.

5. De i stk. 1 omhandlede medlemsstatsmyndigheder og EU-agenturer kan benytte ESP til at søge efter oplysninger om personer eller deres rejsedokumenter i Europoloplysningerne i overensstemmelse med deres adgangsret i henhold til EU-retten og national ret.

Artikel 8

Profiler for brugerne af den europæiske søgeportal

1. Med henblik på at muliggøre brugen af ESP opretter eu-LISA i samarbejde med medlemsstaterne en profil på grundlag af hver kategori af ESP-bruger og formålene med forespørgslerne, i overensstemmelse med de i stk. 2 omhandlede tekniske detaljer og adgangsrettigheder. Hver profil omfatter i overensstemmelse med EU-retten og national ret følgende oplysninger:

a) de datafelter, som skal bruges til at forespørge

b) de EU-informationssystemer, de Europoloplysninger og de INTERPOL-databaser, der skal forespørges i, dem der kan forespørges i, og dem der skal give et svar til brugeren

c) de konkrete oplysninger i EU-informationssystemerne, Europoloplysningerne og INTERPOL-databaserne, der kan forespørges i

d) de kategorier af oplysninger, der kan gives i hvert svar.

2. Kommissionen vedtager gennemførelsesretsakter for at fastlægge de tekniske detaljer for de i stk. 1 omhandlede profiler i overensstemmelse med ESP-brugernes adgangsret i henhold til de retlige instrumenter om EU-informationssystemerne og i henhold til national ret. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

3. De i stk. 1 omhandlede profiler gennemgås regelmæssigt af eu-LISA i samarbejde med medlemsstaterne og mindst én gang årligt, og ajourføres om nødvendigt.

Artikel 9

Forespørgsler

1. ESP-brugerne iværksætter en forespørgsel ved at indsende alfanumeriske eller biometriske oplysninger til ESP. Hvor en forespørgsel er iværksat, foretager ESP samtidigt forespørgsler i ind- og udrejsesystemet, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR, Europoloplysningerne og INTERPOL-databaserne ved hjælp af de oplysninger, som er indsendt af brugeren, og i overensstemmelse med brugerprofilen.

2. De kategorier af oplysninger, der anvendes til at iværksætte en forespørgsel via ESP, svarer til de kategorier af oplysninger vedrørende personer eller rejsedokumenter, der kan anvendes til at foretage forespørgsler i de forskellige EU-informationssystemer, Europoloplysningerne og INTERPOL-databaserne i overensstemmelse med de retlige instrumenter, der regulerer dem.

3. eu-LISA indfører i samarbejde med medlemsstaterne et grænsefladekontroldokument baseret på UMF, der er omhandlet i artikel 38, for ESP.

4. Når en forespørgsel er iværksat af en ESP-bruger, fremkommer ind- og udrejsesystemet, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR, MID, Europoloplysningerne og INTERPOL-databaserne som svar på forespørgslen med de oplysninger, de besidder.

Uden at det berører artikel 20, angiver svaret fra ESP, hvilket EU-informationssystem eller hvilken database oplysningerne stammer fra.

ESP giver ingen oplysninger vedrørende oplysninger i EU-informationssystemer, Europoloplysningerne og de INTERPOL-databaser, som brugeren ikke har adgang til i henhold til gældende EU-ret og national ret.

5. Alle forespørgsler i INTERPOL-databaserne, der iværksættes ved hjælp af ESP, foretages på en sådan måde, at ingen oplysninger afsløres over for ejeren af Interpol-indberetningen.

6. ESP svarer brugeren, så snart oplysninger fra et af EU-informationssystemerne, Europoloplysningerne eller INTERPOL-databaserne foreligger. Disse svar må kun indeholde de oplysninger, som brugeren har adgang til i henhold til EU-retten og national ret.

7. Kommissionen vedtager en gennemførelsesretsakt for at præcisere den tekniske procedure for ESP's forespørgsler i EU-informationssystemerne, Europoloplysningerne og INTERPOL-databaserne samt formatet af svarene fra ESP. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

Artikel 10

Føring af logfiler

1. Uden at det berører artikel 12 og 18 i forordning (EU) 2018/1862, artikel 29 i forordning (EU) 2019/816 og artikel 40 i forordning (EU) 2016/794 fører eu-LISA logfiler over alle databehandlingsaktiviteter i ESP. Disse logfiler indeholder følgende:

a) den medlemsstat eller det EU-agentur, der iværksætter forespørgslen, og den anvendte ESP-profil

b) dato og klokkeslæt for forespørgslen

c) de EU-informationssystemer og Europoloplysninger, der foretages forespørgsler i.

2. Hver medlemsstat fører logfiler over forespørgsler, som foretages af dens myndigheder og disse myndigheders medarbejdere, som er behørigt bemyndiget til at anvende ESP. Hvert EU-agentur fører logfiler over forespørgsler, som foretages af dets behørigt bemyndigede medarbejdere.

3. De i stk. 1 og 2 omhandlede logfiler må kun bruges til overvågning af databeskyttelse, herunder til at kontrollere, hvorvidt en forespørgsel er antagelig, og lovligheden af databehandlingen, og til at garantere datasikkerhed og -integritet. Disse logfiler beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige for overvågningsprocedurerne.

Artikel 11

Alternative procedurer, hvis det er teknisk umuligt at anvende den europæiske søgeportal

1. Hvor det er teknisk umuligt at anvende ESP til at foretage forespørgsler i et eller flere af EU-informationssystemerne eller i CIR på grund af en fejl i ESP, underretter eu-LISA på en automatiseret måde ESP-brugerne af ESP herom.

2. Hvor det er teknisk umuligt at anvende ESP til at foretage forespørgsler i et eller flere af EU-informationssystemerne eller i CIR på grund af en fejl i den nationale infrastruktur i en medlemsstat, underretter den pågældende medlemsstat på en automatiseret måde eu-LISA og Kommissionen herom.

3. I de i denne artikels stk. 1 og 2 omhandlede tilfælde, og indtil den tekniske fejl er rettet, finder forpligtelsen i artikel 7, stk. 2 og 4, ikke anvendelse, og medlemsstaterne tilgår EU-informationssystemerne og CIR direkte, hvor det er krævet af dem i henhold til EU-retten eller national ret.

4. Hvor det er teknisk umuligt at bruge ESP til at foretage forespørgsler i et eller flere af EU-informationssystemerne eller i CIR på grund af funktionssvigt i et EU-agenturs infrastruktur, underretter det pågældende agentur på en automatiseret måde eu-LISA og Kommissionen herom.

KAPITEL III

Den fælles biometriske matchtjeneste

Artikel 12

Fælles biometrisk matchtjeneste

1. Der oprettes en fælles biometrisk matchtjeneste (fælles BMS), der lagrer biometriske skabeloner indhentet fra de i artikel 13 omhandlede biometriske oplysninger, som er lagret i CIR og i SIS, og gør det muligt at foretage forespørgsler med biometriske oplysninger på tværs af flere EU-informationssystemer, med henblik på at understøtte CIR og MID og målene for ind- og udrejsesystemet, VIS, Eurodac, SIS og ECRIS-TCN.

2. Den fælles BMS består af:

a) en central infrastruktur, der erstatter de centrale systemer i henholdsvis ind- og udrejsesystemet, VIS, SIS, Eurodac og ECRIS-TCN i den udstrækning, at den lagrer biometriske skabeloner og giver mulighed for at søge med biometriske oplysninger

b) en sikker kommunikationsinfrastruktur mellem den fælles BMS, det centrale SIS og CIR.

3. eu-LISA udvikler den fælles BMS og sørger for dens tekniske forvaltning.

Artikel 13

Lagring af biometriske skabeloner i den fælles biometriske matchtjeneste

1. Den fælles BMS lagrer de biometriske skabeloner, som det indhenter fra følgende biometriske oplysninger:

a) de oplysninger, der er omhandlet i artikel 20, stk. 3, litra w) og y), bortset fra håndfladeaftryksoplysninger, i forordning (EU) 2018/1862

b) de oplysninger, der er omhandlet i artikel 5, stk. 1, litra b), og stk. 2, i forordning (EU) 2019/816.

De biometriske skabeloner lagres i den fælles BMS logisk adskilt i henhold til det EU-informationssystem, som oplysningerne stammer fra.

2. For hvert i stk. 1 omhandlet sæt oplysninger tilføjer den fælles BMS i hver biometrisk skabelon en henvisning til de EU-informationssystemer, hvor de tilsvarende biometriske oplysninger er lagret, og en henvisning til de konkrete registreringer i disse EU-informationssystemer.

3. Biometriske skabeloner indlæses kun i den fælles BMS efter en automatiseret kvalitetskontrol af de biometriske oplysninger, der er tilføjet et af EU-informationssystemerne, hvilken kvalitetskontrol udføres af den fælles BMS for at sikre, at en minimumsstandard for datakvalitet er opfyldt.

4. Lagringen af de i stk. 1 omhandlede oplysninger skal opfylde de i artikel 37, stk. 2, omhandlede kvalitetsstandarder

5. Kommissionen fastlægger ved hjælp af en gennemførelsesretsakt resultatkravene til og de praktiske ordninger for overvågning af resultaterne for den fælles BMS med henblik på at sikre, at effektiviteten af biometriske søgninger respekterer tidskritiske procedurer, såsom ind- og udrejsekontrol og identifikationer. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

Artikel 14

Søgning efter biometriske oplysninger med den fælles biometriske matchtjeneste

Til at søge efter de biometriske oplysninger, som er lagret i CIR og SIS, anvender CIR og SIS biometriske skabeloner, der er lagret i den fælles BMS. Forespørgsler med biometriske oplysninger finder sted i overensstemmelse med de formål, der er fastsat i denne forordning og i forordning (EF) nr. 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 og (EU) 2019/816.

Artikel 15

Datalagring i den fælles biometriske matchtjeneste

De oplysninger, der er omhandlet i artikel 13, stk. 1 og 2, lagres i den fælles BMS, kun så længe de pågældende biometriske oplysninger lagres i CIR eller SIS. Oplysningerne slettes fra den fælles BMS på en automatiseret måde.

Artikel 16

Føring af logfiler

1. Uden at det berører artikel 12 og 18 i forordning (EU) 2018/1862 og artikel 29 i forordning (EU) 2019/816 fører eu-LISA logfiler over alle databehandlingsaktiviteter i den fælles BMS. Disse logfiler omfatter følgende:

a) medlemsstaten eller EU-agenturet, der har iværksat forespørgslen

b) historikken for oprettelsen og lagringen af biometriske skabeloner

c) de EU-informationssystemer, hvori der foretages forespørgsler med de biometriske skabeloner, der er lagret i den fælles BMS

d) dato og klokkeslæt for forespørgslen

e) typen af biometriske oplysninger, der bruges til at iværksætte forespørgslen

f) resultaterne af forespørgslen og dato og tidspunkt for resultatet.

2. Hver medlemsstat fører logfiler over forespørgsler, som foretages af dens myndigheder og disse myndigheders medarbejdere, som er behørigt bemyndiget til at anvende den fælles BMS. Hvert EU-agentur fører logfiler over forespørgsler, som foretages af dets behørigt bemyndigede medarbejdere.

3. De i stk. 1 og 2 omhandlede logfiler må kun bruges til overvågning af databeskyttelse, herunder til at kontrollere, hvorvidt en forespørgsel er antagelig, og lovligheden af databehandlingen, og til at garantere datasikkerhed og -integritet. Disse logfiler beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige for overvågningsprocedurerne.

KAPITEL IV

Det fælles identitetsregister

Artikel 17

Det fælles identitetsregister

1. Der oprettes et fælles identitetsregister (CIR) med en individuel mappe for hver person, der er registreret i ind- og udrejsesystemet, VIS, ETIAS, Eurodac eller ECRIS-TCN, og indeholdende de i artikel 18 omhandlede oplysninger med henblik på at lette og bistå med korrekt identifikation af personer, der er registreret i ind- og udrejsesystemet, VIS, ETIAS, Eurodac og ECRIS-TCN i overensstemmelse med artikel 20, støtte driften af MID i overensstemmelse med artikel 21 og lette og effektivisere de udpegede myndigheders og Europols adgang til ind- og udrejsesystemet, VIS, ETIAS og Eurodac, når det er nødvendigt for at forebygge, afsløre eller efterforske terrorhandlinger og andre alvorlige strafbare handlinger i overensstemmelse med artikel 22.

2. CIR består af:

a) en central infrastruktur, der erstatter de centrale systemer i henholdsvis ind- og udrejsesystemet, VIS, ETIAS, Eurodac og ECRIS-TCN i den udstrækning, at den lagrer de i artikel 18 omhandledes oplysninger

b) en sikker kommunikationskanal mellem CIR og de medlemsstater og EU-agenturer, der er berettiget til at benytte CIR i overensstemmelse med EU-retten og national ret

c) en sikker kommunikationsinfrastruktur mellem CIR og ind- og udrejsesystemet, VIS, ETIAS, Eurodac og ECRIS-TCN samt med de centrale infrastrukturer i ESP, den fælles BMS og MID.

3. eu-LISA udvikler og står for den tekniske forvaltning af CIR.

4. Hvor det er teknisk umuligt på grund af fejl i CIR at foretage forespørgsel i CIR med henblik på identifikation af en person i henhold til artikel 20, til at påvise flere identiteter i henhold til artikel 21, eller med henblik på at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger i henhold til artikel 22, underretter eu-LISA brugerne af CIR om dette på en automatiseret måde.

5. eu-LISA indfører i samarbejde med medlemsstaterne et grænsefladekontroldokument baseret på UMF, der er omhandlet i artikel 38, for CIR.

Artikel 18

Oplysninger i det fælles identitetsregister

1. CIR lagrer følgende oplysninger — logisk opdelt efter hvilket informationssystem oplysningerne hidrører fra: de oplysninger, der er omhandlet i artikel 5, stk. 1, litra b), og stk. 2, og følgende oplysninger opregnet i artikel 5, stk. 1, litra a), i forordning (EU) 2019/816: efternavn, fornavne, fødselsdato, fødested (by og land), nationalitet eller nationaliteter, køn, eventuelle tidligere navne, pseudonymer eller kaldenavne samt, hvis de forefindes, oplysninger på rejsedokumenter.

2. For hvert af de i stk. 1 omhandlede sæt oplysninger indeholder CIR en henvisning til de EU-informationssystemer, som indeholder oplysningerne.

3. De myndigheder, der tilgår CIR, gør dette i overensstemmelse med deres adgangsrettigheder i henhold til de retlige instrumenter om EU- informationssystemerne og national ret og i overensstemmelse med deres adgangsrettigheder i henhold til denne forordning til de artikel 20, 21 og 22 omhandlede formål.

4. For hvert af de i stk. 1 omhandlede sæt oplysninger indeholder CIR en henvisning til den konkrete registrering i de EU-informationssystemer, som indeholder oplysningerne.

5. Lagringen af de i stk. 1 omhandlede oplysninger opfylder de i artikel 37, stk. 2, omhandlede kvalitetsstandarder.

Artikel 19

Tilføjelse, ændring og sletning af oplysninger i det fælles identitetsregister

1. Hvor der tilføjes, ændres eller slettes oplysninger i Eurodac eller ECRIS-TCN, tilføjes, ændres eller slettes de i artikel 18 omhandlede oplysninger, som er lagret i de individuelle mapper i CIR, tilsvarende på en automatiseret måde.

2. Hvor der oprettes et hvidt eller rødt link i MID i overensstemmelse med artikel 32 eller 33 mellem oplysninger fra to eller flere af de EU-informationssystemer, der udgør CIR, i stedet for at skabe en ny, individuel mappe, tilføjer CIR de nye oplysninger til den individuelle mappe for de sammenkædede oplysninger.

Artikel 20

Adgang til det fælles identitetsregister med henblik på identifikation

1. Forespørgsler i CIR foretages af en politimyndighed i overensstemmelse med stk. 2 og 5 og kun under følgende omstændigheder:

a) hvor en politimyndighed er ude af stand til at identificere en person på grund af fraværet af et rejsedokument eller et andet troværdigt dokument, der beviser den pågældendes identitet

b) hvor der er tvivl om de identitetsoplysninger, som en person har fremlagt

c) hvor der er tvivl om ægtheden af rejsedokumentet eller et andet troværdigt dokument, som en person har fremlagt

d) hvor der er tvivl om identiteten af indehaveren af et rejsedokument eller af et andet troværdigt dokument, eller

e) hvor en person er ude af stand til eller nægter at samarbejde.

Sådanne forespørgsler er ikke tilladt, når der er tale om mindreårige under 12 år, medmindre det er i overensstemmelse med barnets tarv.

2. Hvor en af omstændighederne opregnet i stk. 1 opstår, og en politimyndighed har beføjelse hertil i medfør af nationale lovgivningsmæssige foranstaltninger som omhandlet i stk. 5, kan den udelukkende med henblik på at identificere en person foretage en forespørgsel i CIR med den pågældende persons biometriske oplysninger, som er udtaget på stedet ved en identitetskontrol, forudsat at proceduren blev indledt under tilstedeværelse af den pågældende person.

3. Hvor forespørgslen viser, at oplysningerne for den pågældende person er lagret i CIR, har politimyndigheden adgang til at konsultere de i artikel 18, stk. 1, omhandlede oplysninger.

Hvor de biometriske oplysninger for personen ikke kan anvendes, eller hvor forespørgslen med de pågældende oplysninger slår fejl, foretages forespørgslen med personens identitetsoplysninger kombineret med oplysningerne i rejsedokumenterne eller med de identitetsoplysninger, som den pågældende person har givet.

4. Hvor en politimyndighed har beføjelse hertil i medfør af nationale lovgivningsmæssige foranstaltninger som omhandlet i stk. 6, kan den i tilfælde af en naturkatastrofe, en ulykke eller et terrorangreb og alene med henblik på at identificere ukendte personer, som er ude af stand til at legitimere sig, eller uidentificerede menneskelige rester foretage en forespørgsel i CIR med de pågældende personers biometriske oplysninger.

5. De medlemsstater, som ønsker at gøre brug af den mulighed, der er fastsat i stk. 2, vedtager nationale lovgivningsmæssige foranstaltninger. Medlemsstaterne tager i denne forbindelse hensyn til behovet for at undgå enhver forskelsbehandling af tredjelandsstatsborgere. Sådanne lovgivningsmæssige foranstaltninger skal specificere de præcise formål med identifikationen blandt de formål, der er omhandlet i artikel 2, stk. 1, litra b) og c). De udpeger de kompetente politimyndigheder og fastsætter procedurer, betingelser og kriterier for en sådan kontrol.

6. De medlemsstater, som ønsker at gøre brug af den mulighed, der er fastsat i stk. 4, vedtager nationale lovgivningsmæssige foranstaltninger til fastsættelse af procedurer, betingelser og kriterier.

Artikel 21

Adgang til det fælles identitetsregister til påvisning af flere identiteter

1. Hvor en forespørgsel i CIR resulterer i et gult link i overensstemmelse med artikel 28, stk. 4, har den myndighed, der er ansvarlig for manuel verifikation af forskellige identiteter i overensstemmelse med artikel 29, og udelukkende med henblik på denne verifikation adgang til de i artikel 18, stk. 1 og 2, omhandlede oplysninger, som er lagret i CIR, og som er knyttet til hinanden af et gult link.

2. Hvor en forespørgsel i CIR resulterer i et rødt link i overensstemmelse med artikel 32, har de i artikel 26, stk. 2, omhandlede myndigheder og udelukkende med henblik på bekæmpelse af identitetssvig adgang til de i artikel 18, stk. 1 og 2, omhandlede oplysninger, som er lagret i CIR, og som er knyttet til hinanden af et rødt link.

Artikel 22

Forespørgsler i det fælles identitetsregister med henblik på at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger

1. I særlige tilfælde, hvor der er rimelig grund til at antage, at konsultation af EU-informationssystemerne vil bidrage til forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger, navnlig hvor der er mistanke om, at den mistænkte for, gerningsmanden til eller offeret for en terrorhandling eller anden alvorlig kriminel handling er en person, hvis oplysninger er lagret i Eurodac, kan de udpegede myndigheder og Europol konsultere CIR for at indhente oplysninger om, hvorvidt der findes oplysninger om en bestemt person i Eurodac.

2. Hvor CIR som svar på en forespørgsel angiver, at der findes oplysninger om personen i Eurodac, giver CIR udpegede myndigheder og Europol svar i form af en henvisning som omhandlet i artikel 18, stk. 2, til, som angiver, at Eurodac indeholder matchende oplysninger. Alle svar fra CIR udformes således, at datasikkerheden ikke bringes i fare.

Svaret om, at der foreligger oplysninger i Eurodac om den pågældende person, må kun benyttes til at indgive en anmodning om fuld adgang på de betingelser og efter de procedurer, der er fastsat i det retlige instrument om denne form for adgang.

I tilfælde af et eller flere match anmoder den udpegede myndighed eller Europol om fuld adgang til mindst ét af de informationssystemer, hvor der var et match.

Hvor der undtagelsesvis ikke anmodes om en sådan fuld adgang, registrerer de udpegede myndigheder begrundelsen for ikke at indgive anmodningen, hvilket skal kunne spores i den nationale mappe. Europol registrerer begrundelsen i den relevante mappe.

3. Fuld adgang til oplysningerne i ind- og udrejsesystemet, VIS eller ETIAS med henblik på at forebygge, afsløre og efterforske terrorhandlinger eller andre alvorlige strafbare handlinger er fortsat underlagt betingelserne og procedurerne i de respektive retlige instrumenter, der regulerer denne adgang.

Artikel 23

Lagring af oplysninger i det fælles identitetsregister

1. De i artikel 18, stk. 1, 2 og 4, omhandlede oplysninger slettes fra CIR på en automatiseret måde i overensstemmelse med bestemmelserne om opbevaring af oplysninger i forordning (EU) 2019/816.

2. Den individuelle mappe lagres kun i CIR, så længe de tilsvarende oplysninger er lagret i mindst ét af de EU-informationssystemer, hvis oplysninger er indeholdt i CIR. Oprettelse af et link berører ikke lagringsperioden for hvert af elementerne i de sammenkædede oplysninger.

Artikel 24

Føring af logfiler

1. Uden at det berører artikel 29 i forordning (EU) 2019/816, fører eu-LISA logfiler over alle databehandlingsaktiviteter i CIR i overensstemmelse med nærværende artikels stk. 2, 3 og 4.

2. eu-LISA fører logfiler over alle databehandlingsaktiviteter i CIR i henhold til artikel 20. Disse logfiler omfatter følgende:

a) medlemsstaten eller EU-agenturet, der har iværksat forespørgslen

b) formålet med adgangen for den bruger, der foretager en forespørgsel via CIR

c) dato og klokkeslæt for forespørgslen

d) typen af oplysninger, der bruges til at iværksætte forespørgslen

e) resultaterne af forespørgslen.

3. eu-LISA fører logfiler over alle databehandlingsaktiviteter i CIR i henhold til artikel 21. Disse logfiler omfatter følgende:

a) medlemsstaten eller EU-agenturet, der har iværksat forespørgslen

b) formålet med adgangen for den bruger, der foretager en forespørgsel via CIR

c) dato og klokkeslæt for forespørgslen

d) hvor der oprettes et link, de oplysninger, der bruges til at iværksætte forespørgslen, og resultaterne af forespørgslen med angivelse af det EU-informationssystemet, hvorfra oplysningerne blev modtaget.

4. eu-LISA fører logfiler over alle databehandlingsaktiviteter i CIR i henhold til artikel 22. Disse logfiler omfatter følgende:

a) dato og klokkeslæt for forespørgslen

b) de oplysninger, der bruges til at iværksætte forespørgslen

c) resultaterne af forespørgslen

d) medlemsstaten eller EU-agenturet, der foretager forespørgslen i CIR.

Logfilerne vedrørende sådan adgang kontrolleres regelmæssigt af den kompetente tilsynsmyndighed, der er udpeget i overensstemmelse med artikel 41 i direktiv (EU) 2016/680 eller af den Europæiske Tilsynsførende for Databeskyttelse i overensstemmelse med artikel 43 i forordning (EU) 2016/794, med intervaller på højst seks måneder, for at kontrollere, at de procedurer og betingelser, der er fastsat i artikel 22, stk. 1 og 2, i nærværende forordning, er opfyldt.

5. Hver medlemsstat fører logfiler over forespørgsler, som foretages i henhold til artikel 20, 21 og 22 af dens myndigheder og disse myndigheders medarbejdere, som er behørigt bemyndiget til at anvende CIR. Hvert EU-agentur fører logfiler over forespørgsler, som foretages af dets behørigt bemyndigede medarbejdere i henhold til artikel 21 og 22.

I forbindelse med enhver adgang til CIR i henhold til artikel 22 fører hver medlemsstat desuden følgende logfiler:

a) henvisningen til den nationale mappe

b) formålet med adgangen

c) i overensstemmelse med nationale regler, den unikke brugeridentitet for den embedsmand, der foretog forespørgslen, og for den embedsmand, der bestilte forespørgslen.

6. I overensstemmelse med forordning (EU) 2016/794 fører Europol for enhver adgang til CIR i henhold til nærværende forordnings artikel 22 logfiler over den unikke brugeridentitet for den embedsmand, der foretog forespørgslen, og den embedsmand, der bestilte forespørgslen.

7. De i stk. 2-6 omhandlede logfiler må kun bruges til overvågning af databeskyttelse, herunder til at kontrollere, hvorvidt en forespørgsel er antagelig, og lovligheden af databehandlingen, og til at garantere datasikkerhed og -integritet. Disse logfiler beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige til overvågningsprocedurerne.

8. eu-LISA lagrer de logfiler, der er relateret til historikken for de oplysninger, i individuelle mapper. eu-LISA sletter sådanne logfiler på en automatiseret måde, så snart oplysningerne slettes.

KAPITEL V

Multiidentitetsdetektor

Artikel 25

Multiidentitetsdetektor

1. Der oprettes en multiidentitetsdetektor (MID), der opretter og lagrer identitetsbekræftelsesmapper som omhandlet i artikel 34, der indeholder links mellem oplysninger i de EU-informationssystemer, der indgår i CIR og SIS og muliggør påvisning af flere identiteter, med det dobbelte formål at lette identitetskontrol og bekæmpe identitetssvig, med henblik på at støtte CIR's funktioner og målene for ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN.

2. MID består af:

a) en central infrastruktur, der lagrer links og henvisninger til EU-informationssystemer

b) en sikker kommunikationsinfrastruktur til at forbinde MID med SIS og de centrale infrastrukturer i ESP og CIR.

3. eu-LISA udvikler og står for den tekniske forvaltning af MID.

Artikel 26

Adgang til multiidentitetsdetektoren

1. For så vidt angår den i artikel 29 omhandlede manuelle verifikation af forskellige identiteter gives adgang til de i artikel 34 omhandlede oplysninger, som er lagret i MID, til:

a) SIRENE-kontoret i den medlemsstat, der opretter eller ajourfører en indberetning i overensstemmelse med forordning (EU) 2018/1862

b) de centrale myndigheder i den dømmende medlemsstat ved registrering eller ændring af oplysninger i ECRIS-TCN i overensstemmelse med artikel 5 eller 9 i forordning (EU) 2019/816.

2. Medlemsstatsmyndigheder og EU-agenturer, der har adgang til mindst ét EU-informationssystem, der indgår i CIR, eller til SIS, har adgang til de i artikel 34, litra a) og b), omhandlede oplysninger vedrørende eventuelle røde links, der er omhandlet i artikel 32.

3. Medlemsstatsmyndigheder og EU-agenturer har adgang til de i artikel 33, omhandlede hvide links, hvor de har adgang til de to EU-informationssystemer, der indeholder oplysninger, hvorimellem det hvide link blev oprettet.

4. Medlemsstatsmyndigheder og EU-agenturer har adgang til de i artikel 31 omhandlede grønne links, hvor de har adgang til de to EU-informationssystemer, der indeholder oplysninger, hvorimellem det grønne link blev oprettet, og en forespørgsel i disse informationssystemer har vist et match i forhold til de to sæt sammenkædede oplysninger.

Artikel 27

Påvisning af flere identiteter

1. Der iværksættes påvisning af flere identiteter i CIR og SIS, hvor:

a) der oprettes en indberetning om en person i SIS i overensstemmelse med kapitel VI-IX i forordning (EU) 2018/1862

b) der oprettes en dataregistrering, eller denne ændres, i ECRIS-TCN-systemet i overensstemmelse med artikel 5 eller 9 i forordning (EU) 2019/816.

2. Hvor oplysninger indeholdt i et i stk. 1 omhandlet EU-informationssystem indeholder biometriske oplysninger, anvender CIR og det centrale SIS den fælles BMS til at udføre påvisningen af flere identiteter. Den fælles BMS sammenholder de biometriske skabeloner fra eventuelle nye biometriske oplysninger med de biometriske skabeloner, der allerede er indeholdt i den fælles BMS, til at verificere, om oplysninger tilhørende den samme person allerede er lagret i CIR eller i det centrale SIS.

3. Ud over den i stk. 2 omhandlede proces anvender CIR og det centrale SIS ESP til at søge efter oplysninger lagret i henholdsvis det centrale SIS og CIR ved hjælp af følgende oplysninger:

a) efternavne, fornavne, fødenavne, tidligere anvendte navne og kaldenavne, fødested, fødselsdato, køn og samtlige nationaliteter som omhandlet i artikel 20, stk. 3, i forordning (EU) 2018/1862

b) efternavn, fornavne, fødselsdato, fødested (by og land), nationalitet eller nationaliteter og køn som omhandlet i artikel 5, stk. 1, litra a), i forordning (EU) 2019/816.

4. Ud over den i stk. 2 og 3 omhandlede proces anvender CIR og det centrale SIS ESP til at søge efter oplysninger lagret i henholdsvis det centrale SIS og CIR ved hjælp af rejsedokumentoplysninger.

5. Påvisning af flere identiteter iværksættes kun for at sammenligne oplysninger i ét EU-informationssystem med oplysninger i andre EU-informationssystemer.

Artikel 28

Resultater af påvisningen af flere identiteter

1. Hvor de i artikel 27, stk. 2, 3 og 4, omhandlede forespørgsler ikke giver noget match, fortsætter de i artikel 27, stk. 1, omhandlede procedurer i overensstemmelse med de retlige instrumenter, der regulerer dem.

2. Hvor forespørgslen fastsat i artikel 27, stk. 2, 3 og 4, rapporterer ét eller flere match, opretter CIR og, hvor det er relevant, SIS et link mellem de oplysninger, som er anvendt til at foretage forespørgslen, og de oplysninger, der udløste et match.

Hvor der optræder flere match, oprettes et link mellem alle de oplysninger, der udløste matchet. Hvor der allerede var et link til oplysningerne, udvides det eksisterende link til de oplysninger, der blev anvendt til at foretage forespørgslen.

3. Hvor den i artikel 27, stk. 2, 3 og 4, omhandlede forespørgsel giver et eller flere match, og de tilknyttede mappers identitetsoplysninger er identiske eller ensartede, oprettes et hvidt link i overensstemmelse med artikel 33.

4. Hvor den i artikel 27, stk. 2, 3 og 4, omhandlede forespørgsel giver et eller flere match, og de tilknyttede mappers identitetsoplysninger ikke kan betragtes som værende ensartede, oprettes et gult link i overensstemmelse med artikel 30, og den i artikel 29 omhandlede procedure finder anvendelse.

5. Kommissionen vedtager delegerede retsakter i overensstemmelse med artikel 69 for at fastsætte procedurerne til bestemmelse af, i hvilke tilfælde identitetsoplysninger kan betragtes som værende de samme eller ensartede.

6. Links opbevares i den i artikel 34 omhandlede identitetsbekræftelsesmappe.

7. Kommissionen fastsætter i samarbejde med eu-LISA de tekniske regler for oprettelse af links mellem oplysninger fra forskellige EU-informationssystemer ved hjælp af gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

Artikel 29

Manuel verifikation af forskellige identiteter og de ansvarlige myndigheder

1. Uden at det berører stk. 2, er den ansvarlige myndighed for manuel verifikation af forskellige identiteter:

a) SIRENE-kontoret i medlemsstaten for match, der forekom i forbindelse med oprettelse eller ajourføring af en SIS-indberetning i overensstemmelse med forordning (EU) 2018/1862

b) de centrale myndigheder i den dømmende medlemsstat for match, der forekom i forbindelse med registrering eller ændring af oplysninger i ECRIS-TCN i overensstemmelse med artikel 5 eller 9 i forordning (EU) 2019/816.

MID angiver, hvilken myndighed der er ansvarlig for den manuelle verifikation af de forskellige identiteter i identitetsbekræftelsesmappen.

2. Den myndighed, der er ansvarlig for den manuelle verifikation af de forskellige identiteter i identitetsbekræftelsesmappen, er SIRENE-kontoret i den medlemsstat, som oprettede den indberetning, hvor et link er etableret til oplysninger i en indberetning:

a) om personer, der begæres anholdt med henblik på overgivelse eller udlevering, som omhandlet i artikel 26 i forordning (EU) 2018/1862

b) om savnede eller sårbare personer som omhandlet i artikel 32 i forordning (EU) 2018/1862

c) om personer, der eftersøges med henblik på at yde bistand i forbindelse med retsforfølgning som omhandlet i artikel 34 i forordning (EU) 2018/1862

d) om personer, der er genstand for diskret kontrol, undersøgelseskontrol eller målrettet kontrol som omhandlet i artikel 36 i forordning (EU) 2018/1862.

3. Den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har adgang til de sammenkædede oplysninger, der er indeholdt i de relevante identitetsbekræftelsesmapper, og til de sammenkædede identitetsoplysninger i CIR, og, hvor det er relevant, i SIS. Den vurderer straks de forskellige identiteter. Når denne vurdering er afsluttet, ajourfører den linket i overensstemmelse med artikel 31, 32 og 33 og føjer det straks til identitetsbekræftelsesmappen.

4. Hvor der oprettes mere end ét link, vurderer den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, hvert link særskilt.

5. Hvor oplysninger, der giver et match, allerede er sammenkædet, tager den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, hensyn til de eksisterende links ved vurderingen af oprettelsen af nye links.

Artikel 30

Gult link

1. Hvor manuel verifikation af forskellige identiteter endnu ikke har fundet sted, klassificeres et link mellem oplysninger fra to eller flere EU-informationssystemer som gult i hvert af de følgende tilfælde:

a) de sammenkædede oplysninger har samme biometriske oplysninger, men har ensartede eller forskellige identitetsoplysninger

b) de sammenkædede oplysninger har forskellige identitetsoplysninger, men har samme rejsedokumentoplysninger, og mindst ét af EU-informationssystemerne indeholder ikke nogen biometriske oplysninger om den berørte person

c) de sammenkædede oplysninger har samme identitetsoplysninger, men har forskellige biometriske oplysninger

d) de sammenkædede oplysninger har ensartede eller forskellige identitetsoplysninger og har samme rejsedokumentoplysninger, men har forskellige biometriske oplysninger.

2. Hvor et link er klassificeret som gult i overensstemmelse med stk. 1, finder den i artikel 29 fastsatte procedure anvendelse.

Artikel 31

Grønt link

1. Et link mellem oplysninger fra to eller flere EU-informationssystemer klassificeres som grønt, hvor:

a) de sammenkædede oplysninger har forskellige biometriske oplysninger, men har samme identitetsoplysninger, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til to forskellige personer

b) de sammenkædede oplysninger har forskellige biometriske oplysninger, har ensartede eller forskellige identitetsoplysninger, har samme rejsedokumentoplysninger, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til to forskellige personer

c) de sammenkædede oplysninger har forskellige identitetsoplysninger, men har samme rejsedokumentoplysninger, mindst ét af EU-informationssystemerne indeholder ikke biometriske oplysninger om den berørte person, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til to forskellige personer.

2. Hvor CIR eller SIS forespørges, og hvor der findes et grønt link mellem oplysninger i to eller flere af EU-informationssystemerne, angiver MID, at identitetsoplysningerne for de sammenkædede oplysninger ikke svarer til den samme person.

3. Hvis en medlemsstatsmyndighed har dokumentation, der tyder på, at et grønt link er blevet fejlagtigt registreret i MID, at et grønt link er forældet, eller at oplysninger er blevet behandlet i MID eller EU-informationssystemerne i strid med denne forordning, kontrollerer den de relevante oplysninger, der er lagret i CIR og SIS, og berigtiger eller sletter om nødvendigt straks linket fra MID. Den pågældende medlemsstatsmyndighed informerer straks den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter.

Artikel 32

Rødt link

1. Et link mellem oplysninger fra to eller flere EU-informationssystemer klassificeres som rødt i hvert af de følgende tilfælde:

a) de sammenkædede oplysninger har samme biometriske oplysninger, men har ensartede eller forskellige identitetsoplysninger, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til den samme person på en uberettiget måde

b) de sammenkædede oplysninger har samme, ensartede eller forskellige identitetsoplysninger og samme rejsedokumentoplysninger, men forskellige biometriske oplysninger, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til to forskellige personer, hvoraf mindst én benytter det samme rejsedokument på en uberettiget måde

c) de sammenkædede oplysninger har samme identitetsoplysninger, men forskellige biometriske oplysninger og forskellige eller ingen rejsedokumentoplysninger, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til to forskellige personer på en uberettiget måde

d) de sammenkædede oplysninger har forskellige identitetsoplysninger, men har samme rejsedokumentoplysninger, mindst ét af EU-informationssystemerne indeholder ikke biometriske oplysninger om den berørte person, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til den samme person på en uberettiget måde.

2. Hvor CIR eller SIS forespørges, og hvor der findes et rødt link mellem oplysninger i to eller flere af EU-informationssystemerne, angiver MID de i artikel 34 omhandlede oplysninger. Opfølgning på et rødt link finder sted i overensstemmelse med EU-retten og national ret med eventuelle retlige konsekvenser for den berørte person kun baseret på de relevante oplysninger om denne person. Der må ikke være retlige konsekvenser for den berørte person udelukkende på grundlag af eksistensen af et rødt link.

3. Hvor der oprettes et rødt link mellem oplysninger fra ind- og udrejsesystemet, VIS, ETIAS, Eurodac eller ECRIS-TCN, ajourføres den individuelle mappe, der er lagret i CIR, i overensstemmelse med artikel 19, stk. 2.

4. Uden at det berører bestemmelserne vedrørende behandling af indberetninger i SIS indeholdt i forordning (EU) 2018/1860, (EU) 2018/1861 og (EU) 2018/1862, og uden at det berører de begrænsninger, der er nødvendige for at beskytte sikkerheden og den offentlige orden, forebygge kriminalitet og sikre, at ingen national undersøgelse bringes i fare, underretter den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, hvor der oprettes et rødt link, den pågældende person om, at der er flere ulovlige identitetsoplysninger, og giver personen det i nærværende forordnings artikel 34, litra c), omhandlede enkelte identifikationsnummer, en henvisning til den myndighed, der er ansvarlig for den manuelle verifikation af de i nærværende forordnings artikel 34, litra d), omhandlede forskellige identiteter, og webadressen på den webportal, der er oprettet i overensstemmelse med nærværende forordnings artikel 49.

5. De i stk. 4 omhandlede oplysninger gives skriftligt i form af en standardformular af den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter. Kommissionen fastlægger indholdet og udseendet af denne formular ved hjælp af gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

6. Hvor der oprettes et rødt link, underretter MID de myndigheder, der er ansvarlige for de sammenkædede oplysninger, på en automatiseret måde.

7. Hvis en medlemsstatsmyndighed eller et EU-agentur, der har adgang til CIR eller SIS, har dokumentation, der tyder på, at et rødt link er blevet fejlagtigt registreret i MID, eller at oplysninger er blevet behandlet i MID, CIR eller SIS i strid med denne forordning, kontrollerer denne myndighed eller dette agentur de relevante oplysninger, der er lagret i CIR og SIS, og skal:

a) hvor linket vedrører en af de i artikel 29, stk. 2, omhandlede SIS-indberetninger, omgående underrette det relevante SIRENE-kontor i den medlemsstat, der oprettede SIS-indberetningen

b) i alle andre tilfælde enten berigtige eller slette linket fra MID omgående.

Hvis et SIRENE-kontor kontaktes i henhold til første afsnits litra a), kontrollerer det den dokumentation, der er fremlagt af medlemsstatsmyndigheden eller af EU-agenturet, og, hvor det er relevant, berigtiger eller sletter omgående linket fra MID.

Den medlemsstatsmyndighed, der modtager dokumentationen, underretter straks den medlemsstatsmyndighed, der er ansvarlig for den manuelle kontrol af forskellige identiteter, om enhver relevant berigtigelse eller sletning af et rød link.

Artikel 33

Hvidt link

1. Et link mellem oplysninger fra to eller flere EU-informationssystemer klassificeres som hvidt i hvert af følgende tilfælde:

a) de sammenkædede oplysninger har samme biometriske oplysninger og de samme eller ensartede identitetsoplysninger

b) de sammenkædede oplysninger har samme eller ensartede identitetsoplysninger, samme rejsedokumentoplysninger og mindst ét af EU-informationssystemerne har ingen biometriske oplysninger om den pågældende person

c) de sammenkædede oplysninger har samme biometriske oplysninger, samme rejsedokumentoplysninger og ensartede identitetsoplysninger

d) de sammenkædede oplysninger har samme biometriske oplysninger, men har ensartede eller forskellige identitetsoplysninger, og den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, har konkluderet, at de sammenkædede oplysninger henviser til den samme person på en berettiget måde.

2. Hvor CIR eller SIS forespørges, og hvor der findes et hvidt link mellem oplysninger i to eller flere af EU-informationssystemerne, angiver MID, at identitetsoplysningerne for de sammenkædede oplysninger svarer til den samme person. I svaret fra de forespurgte EU-informationssystemer angives alle de sammenkædede oplysninger for den pågældende person, hvor det er relevant, hvilket giver et match i forhold til de oplysninger, som er sammenkædet af det hvide link, hvis den myndighed, der iværksætter forespørgslen, har adgang til de sammenkædede oplysninger i henhold til EU-retten eller national ret.

3. Hvor der oprettes et hvidt link mellem oplysninger i ind- og udrejsesystemet, VIS, ETIAS, Eurodac eller ECRIS-TCN, ajourføres den individuelle mappe, der er lagret i CIR, i overensstemmelse med artikel 19, stk. 2.

4. Uden at det berører bestemmelserne vedrørende behandling af indberetninger i SIS indeholdt i forordning (EU) 2018/1860, (EU) 2018/1861 og (EU) 2018/1862, og uden at det berører de begrænsninger, der er nødvendige for at beskytte sikkerheden og den offentlige orden, forebygge kriminalitet og sikre, at ingen national efterforskning bringes i fare, underretter den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter, hvor der oprettes et hvidt link efter en manuel verifikation af forskellige identiteter, den pågældende person om, at der er ensartede eller forskellige identitetsoplysninger, og giver personen det i nærværende forordnings artikel 34, litra c), omhandlede enkelte identifikationsnummer, en henvisning til den myndighed, der er ansvarlig for den i nærværende forordnings artikel 34, litra d), omhandlede manuelle verifikation af forskellige identiteter og webadressen på den webportal, der er oprettet i overensstemmelse med nærværende forordnings artikel 49.

5. Hvis en medlemsstatsmyndighed har dokumentation, der tyder på, at et hvidt link er blevet fejlagtigt registreret i MID, at et hvidt link er forældet, eller at oplysninger er blevet behandlet i MID eller EU-informationssystemer i strid med denne forordning, kontrollerer den de relevante oplysninger, der er lagret i CIR og SIS, og berigtiger eller sletter om nødvendigt straks linket fra MID. Den pågældende medlemsstatsmyndighed informerer straks den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter.

6. De i stk. 4 omhandlede oplysninger gives skriftligt ved hjælp af en standardformular af den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter. Kommissionen fastlægger indholdet og udseendet af denne formular ved hjælp af gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

Artikel 34

Identitetsbekræftelsesmappe

Identitetsbekræftelsesmappen skal indeholde følgende oplysninger:

a) de i artikel 30-33 omhandlede links

b) en henvisning til de EU-informationssystemer, hvor de sammenkædede oplysninger opbevares

c) et enkelt identifikationsnummer, som gør det muligt at hente de sammenkædede oplysninger fra det tilsvarende EU-informationssystem

d) den myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter

e) datoen for oprettelse af linket eller for eventuel ajourføring heraf.

Artikel 35

Lagring af oplysninger i multiidentitetsdetektoren

Identitetsbekræftelsesmapperne og oplysningerne deri, herunder links, lagres kun i MID, så længe de sammenkædede oplysninger er lagret i to eller flere EU-informationssystemer. De slettes fra MID på en automatiseret måde.

Artikel 36

Føring af logfiler

1. eu-LISA fører logfiler over alle databehandlingsaktiviteter i MID. Disse logfiler omfatter følgende:

a) den medlemsstat, der iværksætter forespørgslen

b) formålet med brugerens adgang

c) dato og klokkeslæt for forespørgslen

d) typen af oplysninger, der anvendes til at foretage forespørgslen

e) henvisning til de sammenkædede oplysninger

f) historikken for identitetsbekræftelsesmappen.

2. Hver medlemsstat fører logfiler over forespørgsler, som foretages af dens myndigheder og disse myndigheders medarbejdere, som er behørigt bemyndiget til at anvende MID. Hvert EU-agentur fører logfiler over forespørgsler, som foretages af dets behørigt bemyndigede medarbejdere.

3. De i stk. 1 og 2 omhandlede logfiler må kun bruges til overvågning af databeskyttelsen, herunder til at kontrollere, hvorvidt en forespørgsel er antagelig, og lovligheden af databehandlingen, og til at garantere datasikkerhed og -integritet. Disse logfiler beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige for overvågningsprocedurerne.

KAPITEL VI

Foranstaltninger til støtte for interoperabilitet

Artikel 37

Datakvalitet

1. Uden at det berører medlemsstaternes ansvar for så vidt angår kvaliteten af de oplysninger, der indlæses i systemerne, indfører eu-LISA automatiske mekanismer og procedurer for datakvalitetskontrol af de oplysninger, som er lagret i SIS, Eurodac, ECRIS-TCN, den fælles BMS og CIR.

2. eu-LISA indfører fælles mekanismer til evaluering af nøjagtigheden af den fælles BMS, fælles datakvalitetsindikatorer og minimumskvalitetsstandarder til lagring af oplysninger i SIS, Eurodac, ECRIS-TCN, den fælles BMS og CIR.

Kun oplysninger, der opfylder minimumskvalitetsstandarderne, må indføjes i SIS, Eurodac, ECRIS-TCN, den fælles BMS, CIR og MID.

3. eu-LISA aflægger regelmæssigt rapport om de automatiske mekanismer til og procedurer for datakvalitetskontrol og de fælles datakvalitetsindikatorer til medlemsstaterne. eu-LISA aflægger endvidere regelmæssigt rapport til Kommissionen om eventuelle problemer og de heraf berørte medlemsstater. eu-LISA forelægger på anmodning også denne rapport for Europa-Parlamentet og Rådet. Ingen af rapporterne omfattet af dette stykke indeholder nogen personoplysninger.

4. De nærmere detaljer om de automatiske mekanismer til og procedurer for datakvalitetskontrol, de fælles datakvalitetsindikatorer og minimumskvalitetsstandarderne for lagring af oplysninger i SIS, Eurodac, ECRIS-TCN, den fælles BMS og CIR, navnlig vedrørende biometriske oplysninger, fastsættes i gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

5. Et år efter indførelsen af de automatiske mekanismer til og procedurer for datakvalitetskontrol, de fælles datakvalitetsindikatorer og minimumsstandarderne for datakvalitet og hvert år derefter evaluerer Kommissionen medlemsstaternes gennemførelse af datakvalitetskravene og fremsætter alle nødvendige henstillinger. Medlemsstaterne forelægger Kommissionen en handlingsplan for at afhjælpe de mangler, der er konstateret i evalueringsrapporten, og navnlig problemer med datakvalitet hidrørende fra fejlbehæftede oplysninger i EU-informationssystemer. Medlemsstaterne aflægger regelmæssigt rapport til Kommissionen om eventuelle fremskridt i forhold til denne handlingsplan, indtil den er fuldt gennemført.

Kommissionen sender evalueringsrapporten til Europa-Parlamentet, Rådet, Den Europæiske Tilsynsførende for Databeskyttelse, Det Europæiske Databeskyttelsesråd og Den Europæiske Unions Agentur for Grundlæggende Rettigheder, oprettet ved Rådets forordning (EF) nr. 168/2007 ([37]).

Artikel 38

Universelt meddelelsesformat

1. Der indføres hermed en standard for det universelle meddelelsesformat (UMF). Med UMF fastsættes standarder for visse indholdselementer af den grænseoverskridende informationsudveksling mellem informationssystemer, myndigheder og organisationer inden for retlige og indre anliggender.

([37]) Rådets forordning (EF) nr. 168/2007 af 15. februar 2007 om oprettelse af Den Europæiske Unions Agentur for Grundlæggende Rettigheder (EUT L 53 af 22.2.2007, s. 1).

2. UMF-standarden anvendes i forbindelse med udviklingen af Eurodac, ECRIS-TCN, ESP, CIR, MID og, hvis det er hensigtsmæssigt, i forbindelse med eu-LISA's eller et andet EU-agenturs udvikling af nye modeller til informationsudveksling og EU-informationssystemer inden for retlige og indre anliggender.

3. Kommissionen vedtager en gennemførelsesretsakt til fastlæggelse og udvikling af den i denne artikels stk. 1 omhandlede UMF-standard. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

Artikel 39

Centralt register for rapportering og statistik

1. Der oprettes et centralt register for rapportering og statistik (CRRS) med henblik på at støtte målene for SIS, Eurodac og ECRIS-TCN i overensstemmelse med de respektive retlige instrumenter, der regulerer disse systemer, og til at tilvejebringe statistiske oplysninger og analytisk rapportering på tværs af systemerne til politiske, operationelle og datakvalitetsmæssige formål.

2. eu-LISA opretter, gennemfører og hoster CRRS på sine tekniske anlæg, indeholdende de oplysninger og statistikker, der er omhandlet i artikel 74 i forordning (EU) 2018/1862 og artikel 32 i forordning (EU) 2019/816, der holdes logisk adskilt efter EU-informationssystem. Der gives adgang til CRRS via en kontrolleret og sikret adgang og særlige brugerprofiler, udelukkende med henblik på rapportering og statistikker, til de myndigheder, der er omhandlet i artikel 74 i forordning (EU) 2018/1862 og artikel 32 i forordning (EU) 2019/816.

3. eu-LISA anonymiserer oplysningerne og registrerer disse anonymiserede oplysninger i CRRS. Processen for anonymiseringen af oplysningerne skal være automatiseret.

Oplysningerne i CRRS må ikke give mulighed for identifikation af enkeltpersoner.

4. CRRS består af:

a) de nødvendige værktøjer til anonymisering af oplysninger

b) en central infrastruktur bestående af et dataregister med anonymiserede oplysninger

c) en sikker kommunikationsinfrastruktur, der forbinder CRRS til SIS, Eurodac og ECRIS-TCN samt de centrale infrastrukturer i den fælles BMS, CIR og MID.

5. Kommissionen vedtager ved hjælp af en delegeret retsakt, der vedtages efter proceduren i artikel 69, de nærmere regler for driften af CRRS, herunder specifikke sikkerhedsforanstaltninger for behandlingen af personoplysninger i henhold til nærværende artikels stk. 2 og 3 og de sikkerhedsregler, der gælder for registret.

KAPITEL VII

Databeskyttelse

Artikel 40

Dataansvarlig

1. For så vidt angår behandlingen af oplysninger i den fælles BMS, er de medlemsstatsmyndigheder, der er dataansvarlige for henholdsvis Eurodac, SIS og ECRIS-TCN, dataansvarlige i overensstemmelse med artikel 4, nr. 7), i forordning (EU) 2016/679 eller artikel 3, nr. 8), i direktiv (EU) 2016/680 for de biometriske skabeloner fra de i nærværende forordnings artikel 13 omhandlede oplysninger, som de indlæser i de underliggende systemer, og de er ansvarlige for behandlingen af de biometriske skabeloner i den fælles BMS.

2. For så vidt angår behandling af oplysninger i CIR er de medlemsstatsmyndigheder, der er dataansvarlige for henholdsvis Eurodac og ECRIS-TCN, dataansvarlige i overensstemmelse med artikel 4, nr. 7), i forordning (EU) 2016/679 eller artikel 3, nr. 8), i direktiv (EU) 2016/680 for de i nærværende forordnings artikel 18 omhandlede oplysninger, som de indlæser i de underliggende systemer, og de er ansvarlige for behandlingen af de pågældende personoplysninger i CIR.

3. For så vidt angår behandling af oplysninger i MID:

a) er Det Europæiske Agentur for Grænse- og Kystbevogtning dataansvarlig som defineret i artikel 3, nr. 8), i forordning (EU) 2018/1725 for den behandling af personoplysninger, der foretages af den centrale ETIAS-enhed

b) er de medlemsstatsmyndigheder, der tilføjer eller ændrer oplysninger i identitetsbekræftelsesmappen, dataansvarlige i henhold til artikel 4, nr. 7), i forordning (EU) 2016/679 eller artikel 3, nr. 8), i direktiv (EU) 2016/680, og de er ansvarlige for behandlingen af personoplysninger i MID.

4. Med henblik på overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandlingen, har de dataansvarlige adgang til de logfiler, der er omhandlet i artikel 10, 16, 24 og 36, til egenkontrol som omhandlet i artikel 44.

Artikel 41

Databehandler

For så vidt angår behandlingen af personoplysninger i den fælles BMS, CIR og MID, er eu-LISA databehandler som defineret i artikel 3, nr. 12), litra a), i forordning (EU) 2018/1725.

Artikel 42

Behandlingssikkerhed

1. eu-LISA, den centrale ETIAS-enhed, Europol og medlemsstatsmyndighederne sørger for sikkerheden i forbindelse med den behandling af personoplysninger, der finder sted i henhold til denne forordning. eu-LISA, den centrale ETIAS-enhed, Europol og medlemsstatsmyndighederne samarbejder om sikkerhedsrelaterede opgaver.

2. Uden at det berører artikel 33 i forordning (EU) 2018/1725, træffer eu-LISA de nødvendige foranstaltninger for at garantere sikkerheden for interoperabilitetskomponenterne og deres tilhørende kommunikationsinfrastruktur.

3. Navnlig træffer eu-LISA de nødvendige foranstaltninger, herunder en sikkerhedsplan, en forretningskontinuitetsplan og en katastrofeberedskabsplan, med henblik på at:

a) beskytte oplysninger fysisk, herunder ved at udarbejde beredskabsplaner for beskyttelse af kritisk infrastruktur

b) forhindre uautoriserede personers adgang til databehandlingsudstyr og -installationer

c) forhindre uautoriseret læsning, kopiering, ændring og fjernelse af datamedier

d) forhindre uautoriseret indlæsning af oplysninger samt uautoriseret læsning, ændring og sletning af registrerede personoplysninger

e) forhindre uautoriseret behandling af oplysninger samt uautoriseret kopiering, ændring eller sletning af oplysninger

f) forhindre uautoriserede personers brug af automatiserede databehandlingssystemer ved anvendelse af datakommunikationsudstyr

g) sikre, at personer bemyndiget til at få adgang til interoperabilitetskomponenterne kun får adgang til de oplysninger, der er omfattet af deres adgangstilladelse, ved hjælp udelukkende af individuelle brugeridentiteter og fortrolige adgangsmetoder

h) sikre, at det er muligt at kontrollere og fastslå, til hvilke organer personoplysninger må videregives via datatransmissionsudstyr

i) sikre, at det er muligt at kontrollere og fastslå, hvilke oplysninger der er blevet behandlet i interoperabilitetskomponenterne, hvornår, af hvem og til hvilket formål

j) forhindre uautoriseret læsning, kopiering, ændring og sletning af personoplysninger under overførsel af personoplysninger til eller fra interoperabilitetskomponenterne eller under transport af datamedier, navnlig ved hjælp af passende krypteringsteknikker

k) sikre, at de installerede systemer i tilfælde af afbrydelse kan genetableres til normal drift

l) sikre pålidelighed ved at sørge for, at eventuelle funktionsfejl i interoperabilitetskomponenterne indberettes behørigt

m) overvåge effektiviteten af de i dette stykke omhandlede sikkerhedsforanstaltninger og træffe de nødvendige organisatoriske foranstaltninger vedrørende intern overvågning for at sikre overholdelsen af denne forordning og for at vurdere disse sikkerhedsforanstaltninger i lyset af ny teknologiske udvikling.

4. Medlemsstaterne, Europol og den centrale ETIAS-enhed træffer foranstaltninger svarende til dem, der er omhandlet i stk. 3, for så vidt angår sikkerhed, for den behandling af personoplysninger, der udføres af myndigheder med adgangsret til en hvilken som helst af interoperabilitetskomponenterne.

Artikel 43

Sikkerhedshændelser

1. Enhver hændelse, der har eller kan have indvirkning på interoperabilitetskomponenternes sikkerhed eller og kan forårsage skade på eller tab af oplysninger, som er lagret deri, anses for at være en sikkerhedshændelse, navnlig hvor der er sket uautoriseret adgang til oplysninger, eller hvor tilgængeligheden, integriteten og fortroligheden af oplysninger er eller kan være blevet bragt i fare.

2. Sikkerhedshændelser håndteres således, at en hurtig, effektiv og passende reaktion sikres.

3. Uden at det berører anmeldelsen og kommunikationen af et brud på persondatasikkerheden i henhold til artikel 33 i forordning (EU) 2016/679, artikel 30 i direktiv (EU) 2016/680 eller begge, underretter medlemsstaterne straks Kommissionen, eu-LISA, de kompetente tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse om enhver sikkerhedshændelse.

Uden at det berører artikel 34 og 35 i forordning (EU) 2018/1725 og artikel 34 i forordning (EU) 2016/794, underretter den centrale ETIAS-enhed og Europol straks Kommissionen, eu-LISA og Den Europæiske Tilsynsførende for Databeskyttelse om enhver sikkerhedshændelse.

I tilfælde af en sikkerhedshændelse, der vedrører interoperabilitetskomponenternes centrale infrastruktur, underretter eu-LISA straks Kommissionen og Den Europæiske Tilsynsførende for Databeskyttelse.

4. Der gives straks oplysninger om en sikkerhedshændelse, der har eller kan have indvirkning på interoperabilitetskomponenternes drift eller på tilgængeligheden, integriteten og fortroligheden af oplysningerne, til medlemsstaterne, den centrale ETIAS-enhed og Europol, og der rapporteres herom i overensstemmelse med den hændelsesstyringsplan, som eu-LISA skal udforme.

5. De berørte medlemsstater, den centrale ETIAS-enhed, Europol og eu-LISA samarbejder i tilfælde af en sikkerhedshændelse. Kommissionen fastsætter retningslinjer for dette samarbejde ved hjælp af gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

Artikel 44

Egenkontrol

Medlemsstaterne og de relevante EU-agenturer sikrer, at enhver myndighed, der har ret til adgang til interoperabilitetskomponenterne, træffer de foranstaltninger, der er nødvendige for at sikre overholdelsen af denne forordning, og i nødvendigt omfang samarbejder med den nationale tilsynsmyndighed.

De i artikel 40 omhandlede dataansvarlige træffer de nødvendige foranstaltninger for at overvåge, at databehandlingen sker i henhold til denne forordning, herunder ved hyppig kontrol af de i artikel 10, 16, 24 og 36 omhandlede logfiler, og samarbejder, hvor det er nødvendigt, med tilsynsmyndighederne og med Den Europæiske Tilsynsførende for Databeskyttelse.

Artikel 45

Sanktioner

Medlemsstaterne sikrer, at enhver form for misbrug af oplysninger, databehandling eller udveksling af oplysninger i strid med denne forordning er strafbar i overensstemmelse med national ret. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Artikel 46

Erstatningsansvar

1. Uden at det berører retten til erstatning fra den dataansvarlige eller databehandleren og dennes erstatningsansvar i henhold til forordning (EU) 2016/679, direktiv (EU) 2016/680 og forordning (EU) 2018/1725:

a) har enhver person eller medlemsstat, der har lidt materiel eller immateriel skade som følge af en ulovlig behandling af personoplysninger eller enhver anden handling fra en medlemsstats side, der er i strid med denne forordning, ret til erstatning fra den pågældende medlemsstat

b) har enhver person eller medlemsstat, der har lidt materiel eller immateriel skade som følge af en handling fra Europols, Det Europæiske Agentur for Grænse- og Kystbevogtnings eller eu-LISA's side, der er i strid med denne forordning, ret til erstatning fra det pågældende agentur.

Den berørte medlemsstat, Europol, Det Europæiske Agentur for Grænse- og Kystbevogtning eller eu-LISA fritages helt eller delvist for deres erstatningsansvar i medfør af første afsnit, hvis de beviser, at de ikke er skyld i den begivenhed, der forårsagede skaden.

2. Hvis en medlemsstats manglende overholdelse af sine forpligtelser i henhold til denne forordning forårsager skade på interoperabilitetskomponenterne, holdes den pågældende medlemsstat ansvarlig for sådan skade, medmindre og i det omfang eu-LISA eller en anden medlemsstat, der er retligt forpligtet af denne forordning, undlod at træffe rimelige foranstaltninger til at forhindre skaden i at ske eller til at begrænse dens omfang.

3. Erstatningskrav mod en medlemsstat for den i stk. 1 og 2 omhandlede skade behandles efter den sagsøgte medlemsstats nationale ret. Erstatningskrav mod den dataansvarlige eller eu-LISA for den i stk. 1 og 2 omhandlede skade er underlagt de betingelser, der er fastsat i traktaterne.

Artikel 47

Ret til oplysninger

1. Den myndighed, der indsamler personoplysninger, der skal lagres i den fælles BMS, CIR eller MID, giver de personer, hvis oplysninger indsamles, de oplysninger, der er påkrævet i henhold til artikel 13 og 14 i forordning (EU) 2016/679, artikel 12 og 13 i direktiv (EU) 2016/680 og artikel 15 og 16 i forordning (EU) 2018/1725. Myndigheden giver oplysningerne på det tidspunkt, hvor sådanne oplysninger indsamles.

2. Alle oplysninger stilles til rådighed ved anvendelse af et klart og enkelt sprog i en sprogudgave, som den berørte person forstår eller med rimelighed kan forventes at forstå. Dette indebærer, at oplysningerne gives på en alderssvarende måde til registrerede, der er mindreårige.

3. Reglerne om retten til oplysninger i gældende EU-databeskyttelsesregler finder anvendelse på de personoplysninger, der er registreret i ECRIS-TCN og behandles med henblik på denne forordning.

Artikel 48

Ret til indsigt i og berigtigelse og sletning af personoplysninger lagret i MID samt til begrænsning af behandlingen heraf

1. For at kunne udøve sin ret i henhold til artikel 15-18 i forordning (EU) 2016/679, artikel 17-20 i forordning (EU) 2018/1725 og artikel 14, 15 og 16 i direktiv (EU) 2016/80 har enhver person ret til at henvende sig til den kompetente myndighed i en hvilken som helst medlemsstat, som skal undersøge og besvare anmodningen.

2. Den medlemsstat, der behandler en sådan anmodning, svarer uden unødigt ophold og under alle omstændigheder inden for 45 dage efter modtagelsen heraf. Denne periode kan om nødvendigt forlænges med yderligere 15 dage under hensyntagen til anmodningernes kompleksitet og antal. Den medlemsstat, der behandler anmodningen, underretter den registrerede om enhver sådan forlængelse inden for 45 dage efter modtagelsen af anmodningen og angiver begrundelsen for forsinkelsen. Medlemsstaterne kan beslutte, at svarene skal gives af centrale kontorer.

3. Hvis en anmodning om berigtigelse eller sletning af personoplysninger indgives til en anden medlemsstat end den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, kontakter den medlemsstat, som anmodningen er indgivet til, myndighederne i den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, inden for syv dage. Den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, kontrollerer oplysningernes nøjagtighed og lovligheden af databehandlingen uden unødigt ophold og under alle omstændigheder inden for 30 dage efter en sådan kontakt. Denne periode kan om nødvendigt forlænges med yderligere 15 dage under hensyntagen til anmodningernes kompleksitet og antal. Den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, underretter den medlemsstat, der har kontaktet den, om enhver sådan forlængelse sammen med begrundelsen for forsinkelsen. Den berørte person underrettes af den medlemsstat, der har kontaktet myndigheden i den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, om den videre procedure.

4. Hvis en anmodning om berigtigelse eller sletning af personoplysninger indgives til en medlemsstat, hvor den centrale ETIAS-enhed var ansvarlig for den manuelle verifikation af forskellige identiteter, kontakter den medlemsstat, som anmodningen er indgivet til, den centrale ETIAS-enhed inden for syv dage for at anmode den om at afgive udtalelse hurtigst muligt. Den centrale ETIAS-enhed afgiver udtalelse uden unødigt ophold og under alle omstændigheder inden for 30 dage efter at være blevet kontaktet. Denne periode kan om nødvendigt forlænges med yderligere 15 dage under hensyntagen til anmodningernes kompleksitet og antal. Den berørte person underrettes af den medlemsstat, der kontaktede den centrale ETIAS-enhed, om den videre procedure.

5. Hvor det efter en undersøgelse konstateres, at de oplysninger, der er lagret i MID, er ukorrekte eller er blevet registreret ulovligt, berigtiger eller sletter den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, eller, hvor der ikke er en medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, eller hvor den centrale ETIAS-enhed er ansvarlig for den manuelle verifikation af forskellige identiteter, den medlemsstat, som anmodningen er indgivet til, disse oplysninger uden unødigt ophold. Den berørte person underrettes skriftligt om, at vedkommendes oplysninger er blevet berigtiget eller slettet.

6. Hvor oplysninger lagret i MID ændres af en medlemsstat i løbet af deres lagringsperiode, gennemfører denne medlemsstat behandlingen fastsat i artikel 27 og, hvor det er relevant, artikel 29 for at fastslå, om de ændrede oplysninger skal sammenkædes. Hvor behandlingen ikke resulterer i et match, sletter denne medlemsstat oplysningerne i identitetsbekræftelsesmappen. Hvor den automatiserede behandling resulterer i et eller flere match, opretter eller ajourfører denne medlemsstat det relevante link i overensstemmelse med de relevante bestemmelser i denne forordning.

7. Hvor den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, eller i givet fald den medlemsstat, som anmodningen er indgivet til, ikke er enig i, at de oplysninger, som er lagret i MID, er ukorrekte eller er blevet registreret ulovligt, træffer denne medlemsstat en administrativ afgørelse, der straks forklarer den berørte person i skrift, hvorfor den ikke er villig til at berigtige eller slette oplysningerne om vedkommende.

8. Den i stk. 7 omhandlede afgørelse giver også den berørte person oplysninger om muligheden for at anfægte den afgørelse, der er truffet vedrørende anmodningen om indsigt i, berigtigelse af, sletning af eller begrænsning af behandlingen af personoplysninger, og hvor det er relevant, oplysninger om, hvordan der kan indgives et søgsmål eller en klage til de kompetente myndigheder eller til domstolene, samt om eventuel bistand hertil, herunder fra tilsynsmyndighederne.

9. Enhver anmodning om indsigt i, berigtigelse af, sletning af eller begrænsning af behandlingen af personoplysninger skal indeholde de oplysninger, der er nødvendige for at identificere den berørte person. Disse oplysninger må udelukkende anvendes til at muliggøre udøvelsen af de i denne artikel omhandlede rettigheder og slettes umiddelbart efter.

10. Den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, eller i givet fald den medlemsstat, som anmodningen er indgivet til, registrerer skriftligt, at der er indgivet en anmodning om indsigt i, berigtigelse af, sletning af eller begrænsning af behandlingen af personoplysninger, samt hvordan den blev håndteret, og stiller straks registreringen til rådighed for tilsynsmyndighederne.

11. Denne artikel berører ikke begrænsninger og restriktioner af de i denne artikel fastsatte rettigheder i medfør af forordning (EU) 2016/679 og direktiv (EU) 2016/680.

Artikel 49

Webportal

1. Der oprettes en webportal med det formål at lette udøvelsen af retten til adgang til, berigtigelse af, sletning af og begrænsning af behandlingen af personoplysninger.

2. Webportalen indeholder oplysninger om de i artikel 47 og 48 omhandlede rettigheder og procedurer og en brugergrænseflade, der gør det muligt for personer, hvis oplysninger behandles i MID, og som er blevet underrettet om tilstedeværelsen af et rødt link i overensstemmelse med artikel 32, stk. 4, at modtage kontaktoplysninger på den kompetente myndighed i den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter.

3. For at få kontaktoplysninger på den kompetente myndighed i den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, bør den person, hvis oplysninger behandles i MID, indtaste henvisningen til den i artikel 34, litra d), omhandlede myndighed, der er ansvarlig for den manuelle verifikation af forskellige identiteter. Webportalen anvender denne henvisning til at hente kontaktoplysningerne på den kompetente myndighed i den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter. Webportalen skal også indeholde en e-mail-skabelon for at lette kommunikation mellem brugeren af portalen og den kompetente myndighed i den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter. En sådan e-mail skal indeholde et felt til det i artikel 34, litra c), omhandlede enkelte identifikationsnummer for at give den kompetente myndighed i den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, mulighed for at finde frem til de berørte oplysninger.

4. Medlemsstaterne giver eu-LISA kontaktoplysninger på alle de myndigheder, der er kompetente til at behandle og besvare enhver i artikel 47 og 48 omhandlet anmodning, og kontrollerer regelmæssigt, om disse kontaktoplysninger er ajourført.

5. eu-LISA udvikler webportalen og sørger for dens tekniske forvaltning.

6. Kommissionen vedtager en delegeret retsakt i overensstemmelse med artikel 69 for at fastsætte detaljerede bestemmelser om driften af webportalen, herunder brugergrænsefladen, de sprog, som webportalen skal være tilgængelig på, og e-mail-skabelonen.

Artikel 50

Videregivelse af personoplysninger til tredjelande, internationale organisationer og private enheder

Uden at det berører artikel 31 i forordning (EF) nr. 767/2008, artikel 25 og 26 i forordning (EU) 2016/794, artikel 41 i forordning (EU) 2017/2226, artikel 65 i forordning (EU) 2018/1240 og forespørgslerne i INTERPOL-databaserne via ESP i overensstemmelse med nærværende forordnings artikel 9, stk. 5, som overholder bestemmelserne i kapitel V i forordning (EU) 2018/1725 og kapitel V i forordning (EU) 2016/679 må personoplysninger, der er lagret i, behandles af eller tilgås af interoperabilitetskomponenterne, ikke overføres til eller stilles til rådighed for noget tredjeland, nogen international organisation eller nogen privat part.

Artikel 51

Tilsynsmyndighedernes tilsyn

1. Hver medlemsstat sikrer, at tilsynsmyndighederne uafhængigt overvåger lovligheden af den pågældende medlemsstats behandling af personoplysninger i henhold til denne forordning, herunder overførsel af dem til og fra interoperabilitetskomponenterne.

2. Hver medlemsstat sikrer, at de nationale love og administrative bestemmelser, der er vedtaget i henhold til direktiv (EU) 2016/680, også finder anvendelse på politimyndighedernes og de udpegede myndigheders adgang til interoperabilitetskomponenterne, hvor det er relevant, herunder hvad angår rettighederne for de personer, hvis oplysninger der således gives adgang til.

3. Tilsynsmyndighederne sikrer, at der mindst hvert fjerde år foretages en revision af de ansvarlige nationale myndigheders behandling af personoplysninger i forbindelse med denne forordning i overensstemmelse med relevante internationale revisionsstandarder.

Tilsynsmyndighederne offentliggør årligt antallet af anmodninger om berigtigelse, sletning eller begrænsning af behandlingen af personoplysninger, de foranstaltninger, der efterfølgende er truffet, samt antallet af berigtigelser, sletninger og begrænsninger af behandlingen, der er foretaget som følge af anmodninger fra de berørte personer.

4. Medlemsstaterne sikrer, at deres tilsynsmyndigheder har tilstrækkelige ressourcer og ekspertise til at udføre de opgaver, som er tillagt dem i henhold til denne forordning.

5. Medlemsstaterne giver alle de oplysninger, som den tilsynsmyndighed, der er omhandlet i artikel 51, stk. 1, i forordning (EU) 2016/679, anmoder om, herunder navnlig oplysninger om de aktiviteter, der gennemføres i overensstemmelse med deres ansvar i henhold til nærværende forordning. Medlemsstaterne giver de tilsynsmyndigheder, der er omhandlet i artikel 51, stk. 1, i forordning (EU) 2016/679, adgang til deres i nærværende forordnings artikel 10, 16, 24 og 36 omhandlede logfiler og til deres i nærværende forordnings artikel 22, stk. 2, omhandlede begrundelser, og giver dem til enhver tid adgang til alle deres lokaler, som anvendes til interoperabilitetsformål.

Artikel 52

Revision ved Den Europæiske Tilsynsførende for Databeskyttelse

Den Europæiske Tilsynsførende for Databeskyttelse sikrer, at der mindst hvert fjerde år foretages en revision af eu-LISA's, den centrale ETIAS-enheds og Europols aktiviteter til behandling af personoplysninger i forbindelse med denne forordning i overensstemmelse med relevante internationale revisionsstandarder. Europa-Parlamentet, Rådet, eu-LISA, Kommissionen, medlemsstaterne og det berørte EU-agentur tilsendes en rapport om denne revision. eu-LISA, den centrale ETIAS-enhed og Europol har lejlighed til at fremsætte bemærkninger, inden rapporterne vedtages.

eu-LISA, den centrale ETIAS-enhed og Europol udleverer de oplysninger, som Den Europæiske Tilsynsførende for Databeskyttelse anmoder om, giver Den Europæiske Tilsynsførende for Databeskyttelse adgang til alle de dokumenter, denne anmoder om, og til deres i artikel 10, 16, 24 og 36 omhandlede logfiler og giver til enhver tid Den Europæiske Tilsynsførende for Databeskyttelse adgang til alle deres lokaler.

Artikel 53

Samarbejde mellem tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse

1. Tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse, der hver især handler inden for deres respektive beføjelser, samarbejder aktivt inden for rammerne af deres respektive ansvarsområder og sikrer samordnet tilsyn med anvendelsen af interoperabilitetskomponenterne og af de øvrige bestemmelser i denne forordning, navnlig hvis Den Europæiske Tilsynsførende for Databeskyttelse eller en tilsynsmyndighed finder store forskelle mellem medlemsstaternes praksis eller potentielt ulovlige overførsler ved hjælp af kommunikationskanalerne for interoperabilitetskomponenterne.

2. I de i denne artikels stk. 1 omhandlede tilfælde sikres det koordinerede tilsyn som fastsat i artikel 62 i forordning (EU) 2018/1725.

3. Det Europæiske Databeskyttelsesråd sender en fælles rapport om dets aktiviteter i henhold til denne artikel til Europa-Parlamentet, Rådet, Kommissionen, Europol, Det Europæiske Agentur for Grænse- og Kystbevogtning og eu-LISA senest den 12. juni 2021 og derefter hvert andet år. Rapporten indeholder et kapitel om hver medlemsstat, som udarbejdes af den pågældende medlemsstats tilsynsmyndighed.

KAPITEL VIII

Ansvarsområder

Artikel 54

eu-LISA's ansvarsområder under udformnings- og udviklingsfasen

1. eu-LISA sikrer, at de centrale infrastrukturer i interoperabilitetskomponenterne drives i henhold til denne forordning.

2. Interoperabilitetskomponenterne hostes af eu-LISA på dettes tekniske anlæg og leverer de funktionaliteter, der er fastsat i denne forordning, i overensstemmelse med de i artikel 55, stk. 1, omhandlede betingelser for sikkerhed, tilgængelighed, kvalitet og funktionsdygtighed.

3. eu-LISA er ansvarligt for udviklingen af interoperabilitetskomponenterne, for eventuelle tilpasninger, der kræves for at skabe interoperabilitet mellem de centrale systemer i ind- og udrejsesystemet, VIS, ETIAS, SIS, Eurodac, ECRIS-TCN og ESP, den fælles BMS, CIR, MID og CRRS.

eu-LISA har ikke adgang til nogen af de personoplysninger, der behandles gennem ESP, den fælles BMS, CIR og MID, jf. dog artikel 62.

eu-LISA fastlægger udformningen af interoperabilitetskomponenternes fysiske arkitektur, herunder deres kommunikationsinfrastruktur og de tekniske specifikationer og deres udvikling, hvad angår den centrale infrastruktur og den sikre kommunikationsinfrastruktur, der vedtages af bestyrelsen, med forbehold af en gunstig udtalelse fra Kommissionen. eu-LISA gennemfører også de nødvendige tilpasninger af SIS, Eurodac og ECRIS-TCN som følge af etableringen af interoperabilitet og som fastsat i denne forordning.

eu-LISA udvikler og implementerer interoperabilitetskomponenterne så snart som muligt efter ikrafttrædelsen af denne forordning og Kommissionens vedtagelse af de foranstaltninger, der er fastsat i artikel 8, stk. 2, artikel 9, stk. 7, artikel 28, stk. 5 og 7, artikel 37, stk. 4, artikel 38, stk. 3, artikel 39, stk. 5, artikel 43, stk. 5, og artikel 74, stk. 10.

Udviklingsarbejdet omfatter udarbejdelse og gennemførelse af de tekniske specifikationer, afprøvning og overordnet projektstyring og -koordinering.

4. Under udformnings- og udviklingsfasen nedsættes et programstyringsråd bestående af højst 10 medlemmer. Udvalget består af syv medlemmer udpeget af eu-LISA's bestyrelse blandt dets medlemmer eller suppleanter, formanden for den i artikel 71 omhandlede rådgivende gruppe for interoperabilitet, et medlem, der repræsenterer eu-LISA, udpeget af dets administrerende direktør, og et medlem udpeget af Kommissionen. De medlemmer, der udpeges af eu-LISA's bestyrelse, vælges alene fra de medlemsstater, der i henhold til EU-retten er fuldt ud bundet af de retlige instrumenter om udvikling, oprettelse, drift og brug af alle EU-informationssystemerne, og som deltager i interoperabilitetskomponenterne.

5. Programstyringsrådet mødes regelmæssigt og mindst tre gange pr. kvartal. Det sikrer en hensigtsmæssig styring af interoperabilitetskomponenternes udformnings- og udviklingsfase.

Programstyringsrådet indgiver hver måned skriftlige rapporter til eu-LISA's bestyrelse om projektets fremskridt. Programstyringsrådet har ingen beslutningskompetence eller noget mandat til at repræsentere medlemmerne af eu-LISA's bestyrelse.

6. eu-LISA's bestyrelse fastsætter programstyringsrådets forretningsorden, som navnlig indeholder regler om:

a) formandskab

b) mødesteder

c) forberedelse af møder

d) eksperters adgang til møderne

e) kommunikationsplaner, der sikrer, at fraværende medlemmer af bestyrelsen er fuldt ud informeret.

Formandskabet varetages af en medlemsstat, der i henhold til EU-retten er fuldt ud bundet af de retlige instrumenter om udvikling, oprettelse, drift og brug af alle EU-informationssystemerne og som deltager i interoperabilitetskomponenterne.

Alle rejse- og opholdsudgifter afholdt af medlemmerne af programstyringsrådet betales af eu-LISA, og artikel 10 i eu-LISA's forretningsorden finder tilsvarende anvendelse. eu-LISA forestår programstyringsrådets sekretariat.

Den i artikel 71 omhandlede rådgivende gruppe for interoperabilitet mødes regelmæssigt, indtil interoperabilitetskomponenterne idriftsættes. Det aflægger efter hvert møde rapport til programstyringsrådet. Det yder teknisk ekspertise til støtte for programstyringsrådets opgaver og følger op på, hvor langt medlemsstaterne er nået med deres forberedelser.

Artikel 55

eu-LISA's forpligtelser efter idriftsættelsen

1. Efter idriftsættelsen af hver interoperabilitetskomponent er eu-LISA ansvarligt for den tekniske forvaltning af interoperabilitetskomponenternes centrale infrastruktur, herunder deres vedligeholdelse og teknologiske udviklinger. I samarbejde med medlemsstaterne sikrer det, at den bedste disponible teknologi anvendes på grundlag af en cost-benefit-analyse. eu-LISA er også ansvarligt for den tekniske forvaltning og sikring af den i artikel 6, 12, 17, 25 og 39 omhandlede kommunikationsinfrastruktur.

Den tekniske forvaltning af interoperabilitetskomponenterne omfatter alle de opgaver og tekniske løsninger, der er nødvendige for, at interoperabilitetskomponenterne kan fungere og levere uafbrudte tjenester til medlemsstaterne og EU-agenturerne døgnet rundt alle ugens syv dage i henhold til denne forordning. Det omfatter den vedligeholdelse og tekniske udvikling, der er nødvendig for at sikre, at komponenterne fungerer på et tilfredsstillende niveau i forhold til den tekniske kvalitet, særligt hvad angår den tid, der kræves til søgninger i de centrale infrastrukturer i overensstemmelse med de tekniske specifikationer.

Alle interoperabilitetskomponenter udvikles og forvaltes på en sådan måde, at der sikres hurtig, problemfri, effektiv og kontrolleret adgang og fuldstændig, uafbrudt tilgængelighed til komponenterne og de oplysninger, der er lagret i MID, den fælles BMS og CIR, samt at svartiden er i overensstemmelse med de operationelle behov hos medlemsstatsmyndighederne og EU-agenturerne.

2. Uden at det berører artikel 17 i vedtægten for tjenestemænd i Den Europæiske Union, anvender eu-LISA passende regler for tavshedspligt eller tilsvarende fortrolighedskrav i forbindelse med sine medarbejdere, der skal arbejde med oplysninger lagret i interoperabilitetskomponenterne. Denne forpligtelse består fortsat, efter at sådanne medarbejdere er fratrådt deres stilling, eller deres virksomhed er ophørt.

eu-LISA har ikke adgang til nogen af de personoplysninger, der behandles gennem ESP, den fælles BMS, CIR og MID, jf. dog artikel 62.

3. eu-LISA udvikler og vedligeholder en mekanisme til og procedurer for kvalitetskontrol af de oplysninger, der er lagret i den fælles BMS og CIR i overensstemmelse med artikel 37.

4. eu-LISA udfører også opgaver i forbindelse med uddannelse i den tekniske brug af interoperabilitetskomponenterne.

Artikel 56

Medlemsstaternes ansvarsområder

1. Hver medlemsstat er ansvarlig for:

a) forbindelsen til kommunikationsinfrastrukturen i ESP og CIR

b) integration af de eksisterende nationale systemer og infrastrukturer med ESP, CIR og MID

c) organisation, forvaltning, drift og vedligeholdelse af den eksisterende nationale infrastruktur og dens forbindelse til interoperabilitetskomponenterne

d) forvaltning af og ordninger for adgangsretten for de kompetente nationale myndigheders behørigt bemyndigede medarbejdere til ESP, CIR og MID i overensstemmelse med denne forordning og oprettelsen og den regelmæssig ajourføring af en liste over disse medarbejdere og deres profiler

e) vedtagelse af de i artikel 20, stk. 5 og 6, omhandlede lovgivningsmæssige foranstaltninger for at få adgang til CIR i identifikationsøjemed

f) den i artikel 29 omhandlede manuelle verifikation af forskellige identiteter

g) overholdelse af datakvalitetskrav, der er fastsat i henhold til EU-retten

h) overholdelse af reglerne for hvert enkelt EU-informationssystem vedrørende personoplysningers sikkerhed og integritet

i) afhjælpning af eventuelle mangler, der er konstateret i Kommissionens evalueringsrapport om datakvalitet, der er omhandlet i artikel 37, stk. 5.

2. Hver medlemsstat forbinder sine udpegede myndigheder til CIR.

Artikel 57

Europols ansvarsområder

1. Europol sikrer behandlingen af forespørgsler i Europoloplysningerne fra ESP. Europol tilpasser grænsefladen til sit forespørgselssystem (QUEST) til oplysninger på grundlæggende beskyttelsesniveau (BPL) i overensstemmelse hermed.

2. Europol er ansvarligt for at forvalte og tilrettelægge sine behørigt bemyndigede medarbejderes brug af og adgang til ESP og CIR i henhold til denne forordning og for at føre og regelmæssigt ajourføre en liste over disse medarbejdere og deres profiler.

Artikel 58

Den centrale ETIAS-enheds ansvar

Den centrale ETIAS-enhed er ansvarlig for:

a) den manuelle verifikation af forskellige identiteter i overensstemmelse med artikel 29

b) udførelse af påvisning af flere identiteter blandt de oplysninger, der er lagret i ind- og udrejsesystemet, VIS, Eurodac og SIS som omhandlet i artikel 65.

KAPITEL IX

Ændring af andre EU-instrumenter

Artikel 59

Ændring af forordning (EU) 2018/1726

Forordning (EU) 2018/1726 ændres således:

1) Artikel 12 affattes således:

»*Artikel 12*

Datakvalitet

1. Uden at det berører medlemsstaternes ansvar med hensyn til de oplysninger, der indlæses i systemerne under agenturets operationelle ansvar, indfører agenturet under tæt inddragelse af sine rådgivende grupper for alle systemer under agenturets operationelle ansvar automatiserede mekanismer til og procedurer for datakvalitetskontrol, fælles datakvalitetsindikatorer og minimumskvalitetsstandarder for lagring af oplysninger i overensstemmelse med de retlige instrumenter, der regulerer disse informationssystemer, og artikel 37 i Europa-Parlamentets og Rådets forordning (EU) 2019/817 (*) og (EU) 2019/818 (**).

2. Agenturet opretter et centralt register, der kun indeholder anonymiserede oplysninger, med henblik på rapportering og statistikker i overensstemmelse med artikel 39 i forordning (EU) 2019/817 og (EU) 2019/818, uden at det berører særlige bestemmelser i de retlige instrumenter om udvikling, oprettelse, drift og brug af store IT-systemer, der forvaltes af agenturet.

(*) Europa-Parlamentets og Rådets forordning (EU) 2019/817 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende grænser og visum og om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 og (EU) 2018/1861, Rådets beslutning 2004/512/EF og Rådets afgørelse 2008/633/RIA (EUT L 135 af 22.5.2019, s. 27).

(**) Europa-Parlamentets og Rådets forordning (EU) 2019/818 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende politisamarbejde og retligt samarbejde, asyl og migration og om ændring af forordning (EU) 2018/1726, (EU) 2018/1862 og (EU) 2019/816 (EUT L 135 af 22.5.2019, s. 85).«

2) I artikel 19, stk. 1, foretages følgende ændringer:

a) Følgende litra indsættes:

»eea) vedtage rapporter om status med hensyn til udviklingen af interoperabilitetskomponenterne i medfør af artikel 78, stk. 2, i forordning (EU) 2019/817 og artikel 74, stk. 2, i forordning (EU) 2019/818.«

b) Litra ff) affattes således:

»ff) vedtage rapporter om den tekniske funktion af SIS i henhold til artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2018/1861 (*) og artikel 74, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) 2018/1862 (**), af VIS i medfør af artikel 50, stk. 3, i forordning (EF) nr. 767/2008 og artikel 17, stk. 3, i afgørelse 2008/633/RIA, af ind- og udrejsesystemet i medfør af artikel 72, stk. 4, i forordning (EU) 2017/2226, af ETIAS i medfør af artikel 92, stk. 4, i forordning (EU) 2018/1240, af ECRIS-TCN og ECRIS-referencegennemførelsen i medfør af artikel 36, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) 2019/816 (***) og af interoperabilitetskomponenterne i medfør af artikel 78, stk. 3, i forordning (EU) 2019/817 og artikel 74, stk. 3, i forordning (EU) 2019/818

(*) Europa-Parlamentets og Rådets forordning (EU) 2018/1861 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området ind- og udrejsekontrol, om ændring af konventionen om gennemførelse af Schengenaftalen og om ændring og ophævelse af forordning (EF) nr. 1987/2006 (EUT L 312 af 7.12.2018, s. 14).

(**) Europa-Parlamentets og Rådets forordning (EU) 2018/1862 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området politisamarbejde og strafferetligt samarbejde, om ændring og ophævelse af Rådets afgørelse 2007/533/RIA og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1986/2006 og Kommissionens afgørelse 2010/261/EU (EUT L 312 af 7.12.2018, s. 56).

(***) Europa-Parlamentets og Rådets forordning (EU) 2019/816 af 17. april 2019 om oprettelse af et centralt system til bestemmelse af, hvilke medlemsstater der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer (ECRIS-TCN) for at supplere og understøtte det europæiske informationssystem vedrørende strafferegistre, og om ændring af forordning (EU) 2018/1726 (EUT L 135 af 22.5.2019, s. 1).«

c) Litra hh) affattes således:

»hh) vedtage formelle bemærkninger til dets auditrapporter fra Den Europæiske Tilsynsførende for Databeskyttelse udført i henhold til artikel 56, stk. 2, i forordning (EU) 2018/1861, artikel 42, stk. 2, i forordning (EF) nr. 767/2008, artikel 31, stk. 2, i forordning (EU) nr. 603/2013, artikel 56, stk. 2, i forordning (EU) 2017/2226, artikel 67 i forordning (EU) 2018/1240, artikel 29, stk. 2, i forordning (EU) 2019/816 og artikel 52 i forordning (EU) 2019/817 og (EU) 2019/818 og sikre passende opfølgning på disse audits«.

d) Litra mm) affattes således:

»mm) sikre den årlige offentliggørelse af listen over de kompetente myndigheder, der har tilladelse til direkte søgning i oplysningerne i SIS, jf. artikel 41, stk. 8, i forordning (EU) 2018/1861 og artikel 56, stk. 7, i forordning (EU) 2018/1862, sammen med listen over kontorer for de nationale systemer af SIS (N.SIS-kontorer) og SIRENE-kontorer, jf. artikel 7, stk. 3, i forordning (EU) 2018/1861 og artikel 7, stk. 3, i forordning (EU) 2018/1862, samt listen over kompetente myndigheder, jf. artikel 65, stk. 2, i forordning (EU) 2017/2226, listen over kompetente myndigheder, jf. artikel 87, stk. 2, i forordning (EU) 2018/1240, listen over centrale myndigheder, jf. artikel 34, stk. 2, i forordning (EU) 2019/816 og listen over myndigheder, jf. artikel 71, stk. 1, i forordning (EU) 2019/817 og artikel 67, stk. 1, i forordning (EU) 2019/818«.

4) Artikel 22, stk. 4, affattes således:

»4. Europol og Eurojust kan deltage i bestyrelsens møder som observatører, når et spørgsmål vedrørende SIS II i forbindelse med anvendelsen af afgørelse 2007/533/RIA er på dagsordenen.

Det Europæiske Agentur for Grænse- og Kystbevogtning kan deltage i bestyrelsens møder som observatør, når et spørgsmål vedrørende SIS i forbindelse med anvendelsen af forordning (EU) 2016/1624 er på dagsordenen.

Europol kan deltage i bestyrelsens møder som observatør, når et spørgsmål vedrørende VIS i forbindelse med anvendelsen af afgørelse 2008/633/RIA eller et spørgsmål vedrørende Eurodac i forbindelse med anvendelsen af forordning (EU) nr. 603/2013 er på dagsordenen.

Europol kan deltage i bestyrelsens møder som observatør, når et spørgsmål vedrørende ind- og udrejsesystemet i forbindelse med anvendelsen af forordning (EU) 2017/2226 er på dagsordenen eller når et spørgsmål vedrørende ETIAS i forbindelse med forordning (EU) 2018/1240 er på dagsordenen.

Det Europæiske Agentur for Grænse- og Kystbevogtning kan deltage i bestyrelsens møder som observatør, når et spørgsmål vedrørende ETIAS i forbindelse med anvendelsen af forordning (EU) 2018/1240 er på dagsordenen.

Eurojust, Europol og Den Europæiske Anklagemyndighed kan deltage i bestyrelsens møder som observatører, når et spørgsmål vedrørende forordning (EU) 2019/816 er på dagsordenen.

Europol, Eurojust og Det Europæiske Agentur for Grænse- og Kystbevogtning kan deltage i bestyrelsens møder som observatører, når et spørgsmål vedrørende forordning (EU) 2019/817 og (EU) 2019/818 er på dagsordenen.

Bestyrelsen kan indbyde enhver anden person, hvis synspunkt kan være af interesse, til at deltage i dens møder som observatør.«

5) Artikel 24, stk. 3, litra p), affattes således:

»p) fastlæggelsen af fortrolighedskrav, uden at dette berører tjenestemandsvedtægtens artikel 17, for at efterkomme henholdsvis artikel 17 i forordning (EF) nr. 1987/2006, artikel 17 i afgørelse 2007/533/RIA, artikel 26, stk. 9, i forordning (EF) nr. 767/2008, artikel 4, stk. 4, i forordning (EU) nr. 603/2013, artikel 37, stk. 4, i forordning (EU) 2017/2226 og artikel 74, stk. 2, i forordning (EU) 2018/1240, artikel 11, stk. 16, i forordning (EU) 2019/816 og artikel 55, stk. 2, i forordning (EU) 2019/817 og (EU) 2019/818«.

6) Artikel 27 ændres således:

a) I stk. 1 indsættes følgende litra:

»da) Den rådgivende gruppe for interoperabilitet«.

b) Stk. 3 affattes således:

»3. Europol og Eurojust og Det Europæiske Agentur for Grænse- og Kystbevogtning kan hver udpege en repræsentant til Den Rådgivende Gruppe for SIS II.

Europol kan også udpege en repræsentant til de rådgivende grupper for VIS og Eurodac og ind- og udrejsesystemet/ETIAS.

Det Europæiske Agentur for Grænse- og Kystbevogtning kan også udpege en repræsentant til Den Rådgivende Gruppe for ind- og udrejsesystemet/ETIAS.

Eurojust, Europol og Den Europæiske Anklagemyndighed kan hver udpege en repræsentant til den rådgivende gruppe for ECRIS-TCN.

Europol, Eurojust og Det Europæiske Agentur for Grænse- og Kystbevogtning kan hver udpege en repræsentant til den rådgivende gruppe for interoperabilitet.«

Artikel 60

Ændring af forordning (EU) 2018/1862

I forordning (EU) 2018/1862 foretages følgende ændringer:

1) I artikel 3 tilføjes følgende numre:

»18) »ESP«: den europæiske søgeportal, der er oprettet ved artikel 6, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2019/818 (*)

19) »den fælles BMS«: den fælles biometriske matchtjeneste, der er oprettet ved artikel 12, stk. 1, i forordning (EU) 2019/818

20) »CIR«: det fælles identitetsregister, der er oprettet ved artikel 17, stk. 1, i forordning (EU) 2019/818

21) »MID«: den multiidentitetsdetektor, som er oprettet ved artikel 25, stk. 1, i forordning (EU) 2019/818

(*) Europa-Parlamentets og Rådets forordning (EU) 2019/818 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende politisamarbejde og retligt samarbejde, asyl og migration og om ændring af forordning (EU) 2018/1726, (EU) 2018/1862 og (EU) 2019/816 (EUT L 135 af 22.5.2019, s. 85).«

2) I artikel 4 foretages følgende ændringer:

a) Stk. 1, litra b) og c), erstattes af følgende:

»b) et nationalt system (N.SIS) i hver enkelt medlemsstat, der består af de nationale datasystemer, der kommunikerer med det centrale SIS, herunder mindst én national eller delt N.SIS-backup

c) en kommunikationsinfrastruktur mellem CS-SIS, CS-SIS-backup og NI-SIS (»kommunikationsinfrastrukturen«), som danner et krypteret virtuelt netværk forbeholdt SIS-oplysninger og udveksling af oplysninger mellem SIRENE-kontorerne som omhandlet i artikel 7, stk. 2, og

d) en sikker kommunikationsinfrastruktur mellem CS-SIS og de centrale infrastrukturer i ESP, den fælles BMS og MID.«

b) Følgende stykker tilføjes:

»8. Uden at dette berører stk. 1-5, kan der også søges efter SIS-oplysninger om personer og identitetspapirer via ESP.

9. Uden at dette berører stk. 1-5, kan SIS-oplysninger om personer og identitetspapirer også overføres via den i stk. 1, litra d), omhandlede sikre kommunikationsinfrastruktur. Disse overførsler skal begrænses til det omfang, disse oplysninger kræves til de formål, der fremgår af forordning (EU) 2019/818.«

3) I artikel 7 indsættes følgende stykke:

»2a. SIRENE-kontorerne sikrer også den manuelle verifikation af forskellige identiteter i overensstemmelse med artikel 29 i forordning (EU) 2019/818. I det omfang, det er nødvendigt for at udføre denne opgave, har SIRENE-kontorerne adgang til de oplysninger, der er lagret i CIR og MID, til de formål, der er fastsat i artikel 21 og 26 i forordning (EU) 2019/818.«

4) I artikel 12, stk. 1, tilføjes følgende afsnit:

»Medlemsstaterne sikrer, at hver adgang til personoplysninger via ESP også registreres med henblik på at kontrollere, hvorvidt søgningen var lovlig, overvåge databehandlingens lovlighed, udøve egenkontrol samt for dataintegritet og datasikkerhed.«

5) I artikel 44, stk. 1, tilføjes følgende litra:

»f) verifikation af forskellige identiteter og bekæmpelse af identitetssvig, i overensstemmelse med kapitel V i forordning (EU) 2019/818.«

6) Artikel 74, stk. 7, affattes således:

»7. Med henblik på artikel 15, stk. 4, og nærværende artikels stk. 3, 4 og 6, lagrer eu-LISA de i artikel 15, stk. 4, og nærværende artikels stk. 3 omhandlede oplysninger« som ikke må muliggøre identifikation af enkeltpersoner i det centrale register for rapportering og statistik, der er omhandlet i artikel 39 i forordning (EU) 2019/818.

eu-LISA gør det muligt for Kommissionen og de i denne artikels stk. 6 omhandlede organer at modtage skræddersyede rapporter og statistikker. eu-LISA giver på anmodning medlemsstaterne, Kommissionen, Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning adgang til det centrale register for rapportering og statistik i overensstemmelse med artikel 39 i forordning (EU) 2019/818.«

Artikel 61

Ændring af forordning (EU) 2019/816

I forordning (EU) 2019/816 foretages følgende ændringer:

1) I artikel 1 tilføjes følgende litra:

»c) fastsættes de betingelser, hvorunder ECRIS-TCN bidrager til at lette og bistå med korrekt identifikation af personer registreret i ECRIS-TCN på de betingelser og til de formål, der fremgår af artikel 20 i Europa-Parlamentets og Rådets forordning (EU) 2019/818 (*) ved at lagre identitetsoplysninger, rejsedokumentoplysninger og biometriske oplysninger i CIR.

(*) Europa-Parlamentets og Rådets forordning (EU) 2019/818 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende politisamarbejde og retligt samarbejde, asyl og migration og om ændring af forordning (EU) 2018/1726, (EU) 2018/1862 og (EU) 2019/816 (EUT L 135 af 22.5.2019, s. 85).«

2) Artikel 2 affattes således:

»*Artikel 2*

Anvendelsesområde

Denne forordning finder anvendelse på behandling af identitetsoplysninger om tredjelandsstatsborgere, der har været genstand for straffedomme i medlemsstaterne, med henblik på bestemmelse af, i hvilken eller hvilke medlemsstater sådanne straffedomme blev afsagt. Med undtagelse af artikel 5, stk. 1, litra b), nr. ii), finder de bestemmelser i denne forordning, der finder anvendelse på tredjelandsstatsborgere, også anvendelse på unionsborgere, som også er statsborgere i et tredjeland, og som har været genstand for straffedomme i medlemsstaterne. Denne forordning letter og bidrager også til en korrekt identifikation af personer i overensstemmelse med nærværende forordning og med forordning (EU) 2019/818.«

3) I artikel 3 foretages følgende ændringer:

a) Nr. 8) udgår.

b) Følgende numre tilføjes:

»19) »CIR«: det fælles identitetsregister som oprettet ved artikel 17, stk. 1, i forordning (EU) 2019/818+

20) »ECRIS-TCN-oplysninger«: alle de oplysninger, der i overensstemmelse med artikel 5 er lagret i det centrale system og i CIR

21) »ESP«: den europæiske søgeportal som oprettet ved artikel 6, stk. 1 i forordning (EU) 2019/818«.

4) I artikel 4, stk. 1, foretages følgende ændringer:

a) Litra a) affattes således:

»a) et centralt system«.

b) Følgende litra indsættes:

»aa) CIR«.

c) Følgende litra tilføjes:

»e) en kommunikationsinfrastruktur mellem det centrale system og ESP's centrale infrastrukturer og CIR.«

5) I artikel 5 foretages følgende ændringer:

a) I stk. 1 affattes indledningen således:

»1. For hver domfældt tredjelandsstatsborger opretter domsstatens centrale myndighed en datapost i ECRIS-TCN. Dataposten skal indeholde:«.

b) Følgende stykke indsættes:

»1a. CIR indeholder de oplysninger, der er omhandlet i stk. 1, litra b), og følgende oplysninger i stk. 1, litra a): efternavn, fornavne, fødselsdato, fødested (by og land), nationalitet eller nationaliteter, køn, eventuelle tidligere navne, hvis de forefindes pseudonymer eller kaldenavn, hvis det forefindes type og nummer på personens rejsedokumenter, samt navnet på den udstedende myndighed. CIR kan indeholde de oplysninger, der er omhandlet i stk. 3. De resterende ECRIS-TCN-oplysninger lagres i det centrale system.«

6) I artikel 8 foretages følgende ændringer

a) Stk. 1 affattes således:

»1. Hver enkelt datapost lagres i det centrale system og i CIR, lige så længe som oplysningerne vedrørende den berørte persons straffedomme lagres i strafferegisteret.«

b) Stk. 2 affattes således:

»2. Ved udløbet af den i stk. 1 omhandlede lagringsperiode sletter domsstatens centrale myndighed dataposten, herunder fingeraftryksoplysninger og ansigtsbilleder, fra det centrale system og fra CIR. Sletningen sker automatisk, hvor det er muligt, og under alle omstændigheder senest én måned efter udløbet af lagringsperioden.«

7) I artikel 9 foretages følgende ændringer:

a) I stk. 1 erstattes ordene »ECRIS-TCN« af ordene »det centrale system og CIR«.

b) I stk. 2, 3 og 4 erstattes ordene »det centrale system« af ordene »det centrale system og CIR«.

8) Artikel 10, stk. 1, litra j), udgår.

9) I artikel 12, stk. 2, erstattes ordene »det centrale system« af ordene »det centrale system og CIR«.

10) I artikel 13, stk. 2, erstattes ordene »det centrale system« af ordene »det centrale system, CIR«.

11) I artikel 23, stk. 2, erstattes ordene »det centrale system« af ordene »det centrale system og CIR«.

12) Artikel 24 ændres således:

a) Stk. 1 affattes således:

»1. De oplysninger, der er indlæst i det centrale system og i CIR, må kun behandles med henblik på bestemmelse af, hvilke medlemsstater der ligger inde med strafferegisteroplysninger om tredjelandsstatsborgere. Oplysningerne indlæst i CIR behandles også i overensstemmelse med forordning (EU) 2019/818 for at bidrage til at lette og bistå med korrekt identifikation af personer registreret i ECRIS-TCN i overensstemmelse med denne forordning.«

b) Følgende stykke tilføjes:

»3. Uden at det berører stk. 2, er adgang til konsultation af de oplysninger, som er lagret i CIR, desuden forbeholdt de behørigt bemyndigede medarbejdere ved de nationale myndigheder i hver enkelt medlemsstat og de behørigt bemyndigede medarbejdere i de EU-agenturer, der er kompetente med hensyn til de formål, der er fastsat i artikel 20 og 21 i forordning (EU) 2019/818. Sådan adgang skal begrænses til det omfang, oplysningerne er nødvendige for udførelsen af deres opgaver med henblik herpå, og stå i forhold til de tilstræbte mål.«

13) Artikel 32, stk. 2, affattes således:

»2. Med henblik på anvendelsen af denne artikels stk. 1 lagrer eu-LISA de i nævnte stykke omhandlede oplysninger i det centrale register for rapportering og statistik, der er omhandlet i artikel 39 i forordning (EU) 2019/818.«

14) I artikel 31, stk. 1, erstattes ordene »det centrale system« af ordene »det centrale system, CIR og«.

15) Artikel 41, stk. 2, affattes således:

»2. Med hensyn til straffedomme afsagt inden datoen for påbegyndelsen af indlæsning af oplysninger i overensstemmelse med artikel 35, stk. 1, opretter de centrale myndigheder de enkelte dataposter i det centrale system og CIR som følger:

a) Alfanumeriske oplysninger, som skal indlæses i det centrale system og CIR ved udgangen af den i artikel 35, stk. 2, omhandlede periode

b) Fingeraftryksoplysninger, som skal indlæses i CIR inden to år efter idriftsættelsen i overensstemmelse med artikel 35, stk. 4.«

KAPITEL X

Afsluttende bestemmelser

Artikel 62

Rapportering og statistik

1. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og eu-LISA har udelukkende adgang til at konsultere antal forespørgsler pr. ESP-bruger-profil med henblik på rapportering og statistik.

Det må ikke være muligt at identificere enkeltpersoner ud fra oplysningerne.

2. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og eu-LISA har adgang til at konsultere følgende oplysninger vedrørende CIR, udelukkende med henblik på rapportering og statistik:

a) antal forespørgsler med henblik på artikel 20, 21 og 22

b) personens nationalitet, køn og fødselsår

c) rejsedokumenttypen og koden på tre bogstaver for det udstedende land

d) antal søgninger foretaget med og uden biometriske oplysninger.

Det må ikke være muligt at identificere enkeltpersoner ud fra oplysningerne.

3. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og eu-LISA har adgang til at konsultere følgende oplysninger vedrørende MID, udelukkende med henblik på rapportering og statistik:

a) antal søgninger foretaget med og uden biometriske oplysninger

b) antallet af hver type link og de EU-informationssystemer, der indeholder de sammenkædede oplysninger

c) den tidsperiode, i hvilken der var et gult og et rødt link i systemet.

Det må ikke være muligt at identificere enkeltpersoner ud fra oplysningerne.

4. De behørigt bemyndigede medarbejdere hos Det Europæiske Agentur for Grænse- og Kystbevogtning har adgang til at konsultere de oplysninger, der er omhandlet i denne artikels stk. 1, 2 og 3, med henblik på at foretage risikoanalyser og sårbarhedsvurderinger som omhandlet i artikel 11 og 13 i Europa-Parlamentets og Rådets forordning (EU) 2016/1624 ([38]).

5. Europols behørigt bemyndigede medarbejdere har adgang til de oplysninger, der er omhandlet i denne artikels stk. 2 og 3, med henblik på at gennemføre strategiske, tematiske og operationelle analyser som omhandlet i artikel 18, stk. 2, litra b) og c), i forordning (EU) 2016/794.

6. Med henblik på anvendelsen af stk. 1, 2 og 3, lagrer eu-LISA de oplysninger, der er omhandlet i nævnte stykker, i CRSS. Det må ikke være muligt at identificere enkeltpersoner ud fra oplysningerne i CRSS, men oplysningerne skal gøre det muligt for de myndigheder, der er nævnt i stk. 1, 2 og 3, at indhente skræddersyede rapporter og statistikker med henblik på at forbedre effektiviteten af ind- og udrejsekontrollen, bistå myndighederne med at behandle visumansøgninger samt understøtte evidensbaseret politikudformning inden for migration og sikkerhed i Unionen.

7. Den Europæiske Unions Agentur for Grundlæggende Rettigheder får på anmodning stillet relevante oplysninger til rådighed af Kommissionen med henblik på at evaluere denne forordnings indvirkning på grundlæggende rettigheder.

([38]) Europa-Parlamentets og Rådets forordning (EU) 2016/1624 af 14. september 2016 om den europæiske grænse- og kystvagt og om ændring af Europa-Parlamentets og Rådets forordning (EU) 2016/399 og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 863/2007, Rådets forordning (EF) nr. 2007/2004 og Rådets beslutning 2005/267/EF (EUT L 251 af 16.9.2016, s. 1).

Artikel 63

Overgangsperiode for brug af den europæiske søgeportal

1. I en periode på to år fra den dato, hvor ESP påbegynder driften, finder de forpligtelser, der er omhandlet i artikel 7, stk. 2 og 4, ikke anvendelse, og det er frivilligt at anvende ESP.

2. Kommissionen tillægges beføjelser til at vedtage en delegeret retsakt i overensstemmelse med artikel 69 for at ændre denne forordning ved at forlænge den i nærværende artikels stk. 1 omhandlede periode én gang med højst ét år, når en vurdering af gennemførelsen af ESP har vist, at en sådan forlængelse er nødvendig, navnlig i betragtning af den indvirkning, som idriftsættelsen af ESP vil have på tilrettelæggelsen og varigheden af ind- og udrejsekontrol.

Artikel 64

Overgangsperiode for bestemmelserne om adgang til det fælles identitetsregister med henblik på at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger

Artikel 22 finder anvendelse fra datoen for idriftsættelsen af CIR som omhandlet i artikel 68, stk. 3.

Artikel 65

Overgangsperiode for multiidentitetsdetektoren

1. I en periode på et år, efter at eu-LISA har underrettet om afslutningen af den test af MID, der henvises til i artikel 68, stk. 4, litra b), og før idriftsættelsen af MID, er den centrale ETIAS-enhed, ansvarlig for at påvise flere identiteter ved brug af de oplysninger, der er lagret i ind- og udrejsesystemet, VIS, Eurodac og SIS. Påvisning af flere identiteter foretages udelukkende ved hjælp af biometriske oplysninger.

2. Hvor forespørgslen resulterer i et eller flere match, og identitetsoplysningerne i de sammenkædede mapper er ens eller ensartede, oprettes et hvidt link i overensstemmelse med artikel 33.

Hvor forespørgslen resulterer i et eller flere match, og identitetsoplysningerne i de sammenkædede mapper ikke kan anses for at være ensartede, oprettes et gult link i overensstemmelse med artikel 30, og proceduren i artikel 29 finder anvendelse.

Hvor der rapporteres om adskillige match, oprettes et link mellem alle de oplysninger, der udløser et match.

3. Hvor der oprettes et gult link, giver MID den centrale ETIAS-enhed adgang til identitetsoplysningerne i de forskellige EU-informationssystemer.

4. Hvor der oprettes et link til en indberetning i SIS, bortset fra en indberetning oprettet i henhold til artikel 3 i forordning (EU) 2018/1860, artikel 24 og 25 i forordning (EU) 2018/1861 eller artikel 38 i forordning (EU) 2018/1862, giver MID SIRENE-kontoret i den medlemsstat, der oprettede indberetningen, adgang til de identitetsoplysninger, der findes i de forskellige informationssystemer.

5. Den centrale ETIAS-enhed eller i det i denne artikels stk. 4 omhandlede tilfælde SIRENE-kontoret i den medlemsstat, der oprettede indberetningen, har adgang til de oplysninger, der findes i identitetsbekræftelsesmappen, og vurderer de forskellige identiteter og ajourfører linket i overensstemmelse med artikel 31, 32 og 33 og føjer det til identitetsbekræftelsesmappen.

6. Den centrale ETIAS-enhed underretter først Kommissionen i overensstemmelse med artikel 67, stk. 3, når alle gule links er blevet manuelt verificeret og deres status ajourført til enten grønne, hvide eller røde links.

7. Medlemsstaterne bistår om nødvendigt den centrale ETIAS-enhed med at udføre påvisningen af flere identiteter i henhold til denne artikel.

8. Kommissionen tillægges beføjelser til at vedtage en delegeret retsakt i overensstemmelse med artikel 69 for at ændre denne forordning ved at forlænge den i nærværende artikels stk. 1 omhandlede periode med seks måneder med mulighed for forlængelse to gange à hver seks måneder. En sådan forlængelse indrømmes kun efter en vurdering af den forventede fuldførelsestid for påvisning af flere identiteter i henhold til nærværende artikel, som viser, at påvisningen af flere identiteter ikke kan fuldføres før udløbet af perioden i henhold til nærværende artikels stk. 1 eller en igangværende forlængelse og af årsager, der er uafhængige af den centrale ETIAS-enhed, og at der ikke kan anvendes korrigerende foranstaltninger. Vurderingen udføres senest tre måneder før udløbet af en sådan periode eller igangværende forlængelse.

Artikel 66

Omkostninger

1. Omkostningerne til etablering og drift af ESP, den fælles BMS, CIR og MID afholdes over Unionens almindelige budget.

2. Omkostningerne i forbindelse med integrationen af de eksisterende nationale infrastrukturer og deres forbindelse til de nationale ensartede grænseflader samt i forbindelse med hosting af de nationale ensartede grænseflader afholdes over Unionens almindelige budget.

Følgende omkostninger dækkes ikke:

a) Medlemsstaternes projektstyringskontor (møder, tjenesterejser, kontorer)

b) hosting af nationale IT-systemer (lokaler, implementering, el, køling)

c) drift af nationale IT-systemer (operatører og supportaftaler)

d) udformning, udvikling, iværksættelse, drift og vedligeholdelse af nationale kommunikationsnet.

3. Uden at det berører yderligere finansiering til dette formål fra andre kilder i Den Europæiske Unions almindelige budget, anvendes et beløb på 32 077 000 EUR fra det rammebeløb på 791 000 000 EUR, der er fastsat i artikel 5, stk. 5, litra b), i forordning (EU) nr. 515/2014 til dækning af omkostningerne ved gennemførelsen af nærværende forordning som forudset i henhold til nærværende artikels stk. 1 og 2.

4. Ud af det i stk. 3 omhandlede rammebeløb afsættes der 22 861 000 EUR til eu-LISA, 9 072 000 EUR til Europol og 144 000 EUR til Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse (Cepol) til støtte for disse agenturer i forbindelse med udførelsen af deres respektive opgaver i henhold til denne forordning. Denne finansiering gennemføres ved indirekte forvaltning.

5. De udpegede myndigheders omkostninger afholdes af den respektive udpegende medlemsstat. Omkostningerne til at forbinde hver udpeget myndighed med CIR afholdes af hver enkelt medlemsstat.

Europols omkostninger, herunder til forbindelse til CIR, afholdes af Europol.

Artikel 67

Meddelelser

1. Medlemsstaterne underretter eu-LISA om de myndigheder, der er omhandlet i stk. 7, 20, 21 og 26, som kan benytte eller få adgang til henholdsvis ESP, CIR og MID.

Der offentliggøres en konsolideret liste over disse myndigheder i *Den Europæiske Unions Tidende* inden tre måneder fra datoen for de enkelte interoperabilitetskomponenters idriftsættelse i overensstemmelse med artikel 68. Hvor der sker ændringer af listen, offentliggør eu-LISA en ajourført konsolideret liste en gang om året.

2. eu-LISA underretter Kommissionen, når de test, der er omhandlet i artikel 68, stk. 1, litra b), stk. 2, litra b), stk. 3, litra b), stk. 4, litra b), stk. 5, litra b), og stk. 6, litra b), er afsluttet på tilfredsstillende vis.

3. Den centrale ETIAS-enhed underretter Kommissionen, når overgangsperioden, der er fastsat i artikel 65, er afsluttet på vellykket vis.

4. Kommissionen stiller de oplysninger, der er meddelt i henhold til stk. 1, til rådighed for medlemsstaterne og offentligheden via et offentligt websted, der opdateres løbende.

Artikel 68

Idriftsættelse

1. Kommissionen bestemmer, fra hvilken dato ESP skal idriftsættes, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er blevet opfyldt:

a) De foranstaltninger, der er omhandlet i artikel 8, stk. 2, artikel 9, stk. 7, og artikel 43, stk. 5, er blevet vedtaget

b) eu-LISA har erklæret, at en omfattende test af ESP, som det har udført i samarbejde med de medlemsstatsmyndigheder og EU-agenturer, der må anvende ESP, er gennemført på tilfredsstillende vis

c) eu-LISA har valideret de tekniske og juridiske foranstaltninger for at indsamle og fremsende de i artikel 8, stk. 1, omhandlede oplysninger og har underrettet Kommissionen derom.

ESP må kun foretage forespørgsler i INTERPOL-databaserne, når de tekniske ordninger gør det muligt at efterleve artikel 9, stk. 5. Enhver manglende mulighed for at efterleve artikel 9, stk. 5, medfører, at ESP ikke foretager forespørgsler i INTERPOL-databaserne, men må ikke forsinke idriftsættelsen af ESP.

Kommissionen fastsætter den i første afsnit omhandlede dato inden for 30 dage efter vedtagelsen af gennemførelsesretsakten.

2. Kommissionen bestemmer, fra hvilken dato den fælles BMS skal idriftsættes, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er blevet opfyldt:

a) Foranstaltningerne omhandlet i artikel 13, stk. 5, og artikel 43, stk. 5, er blevet vedtaget

b) eu-LISA har meddelt, at en omfattende test af den fælles BMS, som det har udført i samarbejde med medlemsstatsmyndighederne, er afsluttet på tilfredsstillende vis

c) eu-LISA har valideret de tekniske og juridiske foranstaltninger for at indsamle og fremsende de i artikel 13 omhandlede oplysninger og har underrettet Kommissionen derom

d) eu-LISA har meddelt, at den test, der er omhandlet i stk. 5, litra b), er afsluttet på tilfredsstillende vis.

Kommissionen fastsætter den i første afsnit omhandlede dato inden for 30 dage efter vedtagelsen af gennemførelsesretsakten.

3. Kommissionen bestemmer, fra hvilken dato CIR skal idriftsættes, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er blevet opfyldt:

a) Foranstaltningerne i artikel 43, stk. 5, og artikel 74, stk. 10, er blevet vedtaget

b) eu-LISA har meddelt, at en omfattende test af CIR, som det har udført i samarbejde med medlemsstatsmyndighederne, er afsluttet på tilfredsstillende vis.

c) eu-LISA har valideret de tekniske og juridiske foranstaltninger for at indsamle og fremsende de i artikel 18 omhandlede oplysninger og har underrettet Kommissionen derom

d) eu-LISA har meddelt, at den test, der er omhandlet i stk. 5, litra b), er afsluttet på tilfredsstillende vis.

Kommissionen fastsætter den i første afsnit omhandlede dato inden for 30 dage efter vedtagelsen af gennemførelsesretsakten.

4. Kommissionen bestemmer, fra hvilken dato MID skal idriftsættes, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er opfyldt:

a) De foranstaltninger, der er omhandlet i artikel 28, stk. 5, artikel 28, stk. 7, artikel 32, stk. 5, artikel 33, stk. 6, artikel 43, stk. 5, og artikel 49, stk. 6, er blevet vedtaget

b) eu-LISA har erklæret, at en omfattende test af MID, som det har udført i samarbejde med medlemsstatsmyndighederne og den centrale ETIAS-enhed, er afsluttet på tilfredsstillende vis

c) eu-LISA har valideret de tekniske og juridiske foranstaltninger for at indsamle og fremsende de i artikel 34 omhandlede oplysninger og har underrettet Kommissionen derom

d) den centrale ETIAS-enhed har underrettet Kommissionen i overensstemmelse med artikel 67, stk. 3

e) eu-LISA har meddelt, at de tests, der er omhandlet i stk. 1, litra b), stk. 2, litra b), stk. 3, litra b), og stk. 5, litra b), er afsluttet på tilfredsstillende vis.

Kommissionen fastsætter den i første afsnit omhandlede dato inden for 30 dage efter vedtagelsen af gennemførelsesretsakten.

5. Kommissionen beslutter ved hjælp af gennemførelsesretsakter, fra hvilken dato de automatiske kvalitetskontrolmekanismer og -procedurer, de fælles datakvalitetsindikatorer og minimumsstandarder for datakvalitet skal anvendes, når følgende betingelser er opfyldt:

a) Foranstaltningerne i artikel 37, stk. 4, er vedtaget

b) eu-LISA har erklæret, at den omfattende test af de automatiske kvalitetskontrolmekanismer og -procedurer, de fælles datakvalitetsindikatorer og minimumsstandarder for datakvalitet, som det har udført i samarbejde med medlemsstatsmyndighederne, er afsluttet på tilfredsstillende vis.

Kommissionen fastsætter den i første afsnit omhandlede dato inden for 30 dage efter vedtagelsen af gennemførelsesretsakten.

6. Kommissionen beslutter, fra hvilken dato CRRS skal idriftsættes, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er opfyldt:

a) Foranstaltningerne i artikel 39, stk. 5, og artikel 43, stk. 5, er vedtaget

b) eu-LISA har meddelt, at den omfattende test af CRRS, som det har udført i samarbejde med medlemsstatsmyndighederne, er afsluttet på tilfredsstillende vis.

c) eu-LISA har valideret de tekniske og juridiske foranstaltninger for at indsamle og fremsende de i artikel 39 omhandlede oplysninger og har underrettet Kommissionen derom.

Kommissionen fastsætter den i første afsnit omhandlede dato inden for 30 dage efter vedtagelsen af gennemførelsesretsakten.

7. Kommissionen meddeler Europa-Parlamentet og Rådet resultaterne af de tests, som er udført i henhold til stk. 1, litra b), stk. 2, litra b), stk. 3, litra b), stk. 4, litra b), stk. 5, litra b), og stk. 6, litra b).

8. Medlemsstaterne, den centrale ETIAS-enhed og Europol begynder at bruge hver af interoperabilitetskomponenterne fra den dato, der fastsættes af Kommissionen i overensstemmelse med henholdsvis stk. 1, 2, 3 og 4.

Artikel 69

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 28, stk. 5, artikel 39, stk. 5, artikel 49, stk. 6, artikel 63, stk. 2, og artikel 65, stk. 8, tillægges Kommissionen for en periode på fem år fra den 11. juni 2019. Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

3. Den i artikel 28, stk. 5, artikel 39, stk. 5, artikel 49, stk. 6, artikel 63, stk. 2, og artikel 65, stk. 8, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 28, stk. 5, artikel 39, stk. 5, artikel 49, stk. 6, artikel 63, stk. 2, og artikel 65, stk. 8, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 70

Udvalgsprocedure

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

Afgiver udvalget ikke nogen udtalelse, vedtager Kommissionen ikke udkastet til gennemførelsesretsakt, og artikel 5, stk. 4, tredje afsnit, i forordning (EU) nr. 182/2011 finder anvendelse.

Artikel 71

Rådgivende gruppe

eu-LISA nedsætter en rådgivende gruppe for interoperabilitet. Under projekterings- og udviklingsfasen af interoperabilitetskomponenterne finder artikel 54, stk. 4, 5 og 6, anvendelse.

Artikel 72

Uddannelse

eu-LISA udfører opgaver vedrørende uddannelse i den tekniske anvendelse af interoperabilitetskomponenterne i overensstemmelse med forordning (EU) 2018/1726.

Medlemsstatsmyndighederne og EU-agenturerne sørger for passende uddannelsesprogrammer vedrørende datasikkerhed, datakvalitet, databeskyttelsesregler og procedurerne for databehandling samt forpligtelsen til at informere i henhold til artikel 32, stk. 4, artikel 33, stk. 4, og artikel 47 for deres medarbejdere, der har beføjelse til at behandle oplysninger ved brug af interoperabilitetskomponenterne.

Hvor det er hensigtsmæssigt, tilrettelægges der fælles uddannelseskurser på EU-plan med henblik på at forbedre samarbejdet og udveksle bedste praksis mellem medarbejderne fra de medlemsstatsmyndigheder og EU-agenturer, der har beføjelse til at behandle oplysninger ved brug af interoperabilitetskomponenterne. Der lægges særlig vægt på processen med påvisning af flere identiteter, herunder den manuelle verifikation af forskellige identiteter og det deraf følgende behov for at opretholde passende sikkerhedsforanstaltninger for de grundlæggende rettigheder.

Artikel 73

Praktisk vejledning

Kommissionen udarbejder i tæt samarbejde med medlemsstaterne, eu-LISA og andre relevante EU-agenturer en praktisk vejledning i gennemførelsen og forvaltningen af interoperabilitetskomponenter. Den praktiske vejledning skal indeholde tekniske og operationelle retningslinjer, anbefalinger og bedste praksis. Kommissionen vedtager vejledningen i form af en henstilling.

Artikel 74

Overvågning og evaluering

1. eu-LISA sikrer, at der er indført procedurer med henblik på at følge udviklingen af interoperabilitetskomponenterne og deres forbindelse til den nationale ensartede grænseflade i lyset af planlægnings- og omkostningsmålene og med henblik på at følge interoperabilitetskomponenternes funktion i lyset af målene for tekniske resultater, omkostningseffektivitet, sikkerhed og tjenestens kvalitet.

2. Senest den 12. december 2019 og derefter hver sjette måned under udviklingsfasen for interoperabilitetskomponenterne forelægger eu-LISA Europa-Parlamentet og Rådet en rapport om status over udviklingen af interoperabilitetskomponenterne samt deres forbindelse til den nationale ensartede grænseflade. Når udviklingen er tilendebragt, forelægges Europa-Parlamentet og Rådet en rapport, som i detaljer forklarer, hvordan målene, navnlig vedrørende planlægning og omkostninger, blev opfyldt, samt angiver grundene til eventuelle afvigelser.

3. Fire år efter idriftsættelsen af de enkelte interoperabilitetskomponenter i overensstemmelse med artikel 68 og derefter hvert fjerde år forelægger eu-LISA Europa-Parlamentet, Rådet og Kommissionen en rapport om, hvordan interoperabilitetskomponenterne fungerer teknisk set, herunder deres sikkerhed.

4. Derudover udarbejder Kommissionen et år efter hver rapport fra eu-LISA en samlet evaluering af interoperabilitetskomponenterne, herunder:

a) en vurdering af denne forordnings anvendelse

b) en gennemgang af de opnåede resultater set i forhold til denne forordnings mål og dens indvirkning på de grundlæggende rettigheder, herunder navnlig en vurdering af interoperabilitetskomponenternes indvirkning på retten til ikkeforskelsbehandling

c) en vurdering af webportalens funktion, herunder tal vedrørende brugen af webportalen og antallet af anmodninger, der er behandlet

d) en vurdering af den fortsatte gyldighed af de underliggende begrundelser for interoperabilitetskomponenterne;

e) en vurdering af sikkerheden ved interoperabilitetskomponenterne

f) en vurdering af anvendelsen af CIR med henblik på identifikation

g) en vurdering af anvendelsen af CIR med henblik på at forebygge, afsløre eller efterforske terrorhandlinger og andre alvorlige strafbare handlinger

h) en vurdering af eventuelle konsekvenser, herunder eventuelle uforholdsmæssigt store virkninger for trafikstrømmen ved grænseovergangssteder, og konsekvenser med budgetmæssige virkninger for Unionens almindelige budget

i) en vurdering af søgninger i INTERPOL-databaserne via ESP, inklusive oplysninger om antallet af match i INTERPOL-databaserne og oplysninger om eventuelle problemer.

Den samlede evaluering i henhold til dette stykkes første afsnit omfatter eventuelle nødvendige henstillinger. Kommissionen sender evalueringsrapporten til Europa-Parlamentet, Rådet, Den Europæiske Tilsynsførende for Databeskyttelse og Den Europæiske Unions Agentur for Grundlæggende Rettigheder.

5. Senest den 12. juni 2020 og hvert år derefter, indtil Kommissionens i artikel 68 omhandlede gennemførelsesretsakter er vedtaget, forelægger Kommissionen en rapport for Europa-Parlamentet og Rådet om status med hensyn til forberedelserne til den fuldstændige gennemførelse af denne forordning. Denne rapport indeholder også detaljerede oplysninger om de afholdte udgifter og oplysninger om eventuelle risici, der kan have indvirkning på de samlede omkostninger.

6. To år efter idriftsættelsen af MID i overensstemmelse med artikel 68, stk. 4, udarbejder Kommissionen en undersøgelse af MID's indvirkning på retten til ikkeforskelsbehandling. Efter denne første rapport er undersøgelsen af virkningen af MID's indvirkning på retten til ikkeforskelsbehandling en del af den undersøgelse, der er omhandlet i nærværende artikels stk. 4, litra b).

7. Medlemsstaterne og Europol giver eu-LISA og Kommissionen de oplysninger, som er nødvendige for at udarbejde de i stk. 3-6 omhandlede rapporter. Disse oplysninger må ikke påvirke arbejdsmetoder negativt eller omfatte oplysninger, som afslører kilder, medarbejdere eller undersøgelser hos de udpegede myndigheder.

8. eu-LISA sender Kommissionen de oplysninger, der er nødvendige for at foretage den i stk. 4 omhandlede samlede evaluering.

9. Hver medlemsstat og Europol udarbejder under overholdelse af national ret om offentliggørelse af følsomme oplysninger, og uden at det berører de begrænsninger, der er nødvendige for at beskytte sikkerheden og den offentlige orden, forebygge kriminalitet og sikre, at ingen nationale undersøgelser bringes i fare, årsrapporter om, hvor effektiv adgangen til oplysninger lagret i CIR har været med henblik på at forebygge, afsløre eller efterforske terrorhandlinger og andre alvorlige strafbare handlinger, indeholdende oplysninger og statistikker om:

a) det nøjagtige formål med konsultationen, herunder hvilke typer terrorhandlinger eller andre alvorlige strafbare handlinger der var tale om

b) den rimelige begrundelse for en begrundet mistanke om, at en mistænkt, en gerningsmand eller et offer er omfattet af forordning (EU) nr. 603/2013

c) antallet af anmodninger om adgang til CIR med henblik på at forebygge, afsløre og efterforske terrorhandlinger eller andre alvorlige strafbare handlinger

d) antal og type af sager, der har ført til korrekt identifikation

e) behovet for og anvendelsen af undtagelserne for hastende tilfælde, herunder de tilfælde, hvor den hastende karakter ikke blev accepteret ved den efterfølgende kontrol, der gennemføres af det centrale adgangspunkt.

Medlemsstaternes og Europols årlige rapporter sendes til Kommissionen senest den 30. juni i det efterfølgende år.

10. Der stilles en teknisk løsning til rådighed for medlemsstaterne med henblik på at forvalte de i artikel 22 omhandlede anmodninger om adgang og lette indsamlingen af oplysninger i henhold til denne artikels stk. 7 og 9 med henblik på udarbejdelse af de i nævnte stykker omhandlede rapporter og statistikker. Kommissionen vedtager gennemførelsesretsakter med henblik på at fastlægge specifikationerne for de tekniske løsninger. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 70, stk. 2.

Artikel 75

Ikrafttræden og anvendelse

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordnings bestemmelser vedrørende ESP finder anvendelse fra den dato, der er fastlagt af Kommissionen i overensstemmelse med artikel 68, stk. 1.

Denne forordnings bestemmelser vedrørende den fælles BMS finder anvendelse fra den dato, der er fastlagt af Kommissionen i overensstemmelse med artikel 68, stk. 2.

Denne forordnings bestemmelser vedrørende CIR finder anvendelse fra den dato, der er fastlagt af Kommissionen i overensstemmelse med artikel 68, stk. 3.

Denne forordnings bestemmelser vedrørende MID finder anvendelse fra den dato, der er fastlagt af Kommissionen i overensstemmelse med artikel 68, stk. 4.

Denne forordnings bestemmelser vedrørende de automatiske kvalitetskontrolmekanismer og -procedurer, de fælles datakvalitetsindikatorer og minimumsstandarderne for datakvalitet finder anvendelse fra de respektive datoer, der er fastlagt af Kommissionen i overensstemmelse med artikel 68, stk. 5.

Denne forordnings bestemmelser vedrørende CRRS finder anvendelse fra den dato, der er fastlagt af Kommissionen i overensstemmelse med artikel 68, stk. 6.

Artikel 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71 og 73 og artikel 74, stk. 1, finder anvendelse fra den 11. juni 2019.

Denne forordning finder anvendelse med hensyn til Eurodac fra den dato, hvor omarbejdningen af Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 finder anvendelse.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i medlemsstaterne i overensstemmelse med traktaterne.

Udfærdiget i Bruxelles, den 20. maj 2019.

På Europa-Parlamentets vegne	*På Rådets vegne*
A. TAJANI	G. CIAMBA
Formand	*Formand*