EUROPA-
KOMMISSIONEN

Strasbourg, den 12.12.2017
COM(2017) 793 final

2017/0351 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om fastsættelse af en ramme for interoperabiliteten mellem EU-informationssystemer (grænser og visum) og om ændring af Rådets afgørelse 2004/512/EF, forordning (EF) nr. 767/2008, Rådets afgørelse 2008/633/RIA, forordning (EU) 2016/399 og forordning (EU) 2017/2226

{SWD(2017) 473 final} - {SWD(2017) 474 final}

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse

I de seneste tre år har EU oplevet en stigning i antallet af irregulære passager af EU's grænser og en ny og voksende trussel mod den indre sikkerhed, således som rækken af terrorangreb viser. EU-borgerne forventer, at ind-og udrejsekontrollen ved de ydre grænser af personer og kontrollerne inden for Schengenområdet er effektive, så det er muligt at sikre en effektiv migrationsstyring og bidrage til den interne sikkerhed. Disse udfordringer har i højere grad sat fokus på det presserende behov for at slutte op om og styrke EU's informationsværktøjer til grænseforvaltning, migration og sikkerhed.

Informationsstyringen i EU kan og skal gøres mere effektiv under fuld overholdelse af de grundlæggende rettigheder, herunder navnlig retten til beskyttelse af personoplysninger, for bedre at kunne beskytte EU's ydre grænser, forbedre migrationsstyringen og øge den interne sikkerhed til gavn for alle borgere. Der findes allerede en række informationssystemer på EU-plan, og flere systemer er under udvikling, som kan give grænsevagter, immigrationsmyndigheder og retshåndhævende myndigheder relevante oplysninger om personer. For at denne støtte kan være effektiv, skal oplysningerne fra EU's informationssystemer være fuldstændige, nøjagtige og pålidelige. Der er dog strukturelle mangler i EU informationsstyringsstruktur. De nationale myndigheder står over for et komplekst landskab af forskelligt regulerede informationssystemer. Desuden er dataforvaltningsstrukturen for grænser og sikkerhed fragmenteret, da oplysningerne opbevares særskilt i systemer, der ikke er koblet sammen. Dette fører til informationshuller. Som følge deraf er **de forskellige informationssystemer på EU-plan i øjeblikket ikke interoperable** – dvs. de er ikke i stand til at udveksle data og dele oplysninger, så myndighederne og de kompetente embedsmænd har de oplysninger, de har brug for, når og hvor de har brug for dem. Interoperabilitet mellem informationssystemer på EU-plan kan bidrage væsentligt til at lukke de nuværende informationshuller, hvor personer, herunder dem, der muligvis er involveret i terrorvirksomhed, kan blive registreret i forskellige, ikkesammenkoblede databaser under forskellige kaldenavne.

I april 2016 fremlagde Kommissionen en **meddelelse om stærkere og mere intelligente informationssystemer for grænser og sikkerhed**[1] for at rette op på en række strukturelle mangler i forbindelse med informationssystemer[2]. Meddelelsen fra april 2016 skulle være et udgangspunkt for drøftelser om, hvordan informationssystemer i EU vil kunne forbedre både forvaltningen af de ydre grænser og den indre sikkerhed i EU. **Rådet** anerkendte for sit eget vedkommende tilsvarende det presserende behov for at handle på dette område. I juni 2016 godkendte det en **køreplan til styrkelse af informationsudveksling og informationsstyring**, herunder interoperabilitetsløsninger på området for retlige og indre anliggender[3]. Formålet med køreplanen var at støtte de operationelle undersøgelser og hurtigt kunne give aktører i første række – såsom politibetjente, grænsevagter, offentlige anklagere,

[1] COM(2016) 205 af 6.4.2016.

[2] 1) suboptimale funktioner i de eksisterende informationssystemer 2) informationshuller i EU's dataforvaltningsstruktur 3) et komplekst landskab af forskelligt regulerede informationssystemer og 4) en fragmenteret dataforvaltningsstruktur for grænser og sikkerhed, hvor oplysningerne lagres særskilt i systemer, der ikke er koblet sammen, hvilket fører til informationshuller.

[3] Køreplan af 6. juni 2016 til styrkelse af informationsudveksling og informationsstyring, herunder interoperabilitetsløsninger på området for retlige og indre anliggender – 9368/1/16 REV 1.

immigrationsmedarbejdere og andre – omfattende og aktuelle oplysninger af høj kvalitet, så de kan samarbejde og træffe effektive foranstaltninger. **Europa-Parlamentet** har også opfordret til handling på området. I sin beslutning af juli 2016[4] om Kommissionens arbejdsprogram for 2017 opfordrede Europa-Parlamentet Kommissionen til at fremlægge "*forslag til at forbedre og udvikle eksisterende informationssystemer, løse problemet med manglende oplysninger og gå i retning af interoperabilitet samt forslag om obligatorisk udveksling af oplysninger på EU-plan ledsaget af nødvendige databeskyttelsesregler*". I kommissionsformand Jean-Claude Junckers tale om Unionens tilstand i september 2016[5] og i konklusionerne fra Det Europæiske Råds møde i december 2016[6] blev det understreget, at det var vigtigt at afhjælpe de nuværende mangler i informationsstyringen og at forbedre de eksisterende informationssystemers interoperabilitet.

I juni 2016 nedsatte Kommissionen som en opfølgning på meddelelsen fra april 2016 **en ekspertgruppe på højt niveau om informationssystemer og interoperabilitet**[7] med henblik på at løse de juridiske, tekniske og driftsmæssige udfordringer i at øge interoperabiliteten mellem centrale EU-systemer for grænser og sikkerhed, herunder deres nødvendighed, tekniske gennemførlighed, proportionalitet og konsekvenser for databeskyttelsen. Den **endelige rapport** fra ekspertgruppen på højt niveau blev offentliggjort den 11. maj 2017[8]. Den indeholdt en række anbefalinger for at styrke og udvikle EU's informationssystemer og deres interoperabilitet. Den Europæiske Unions Agentur for Grundlæggende Rettigheder, Den Europæiske Tilsynsførende for Databeskyttelse og EU's antiterrorkoordinator deltog alle aktivt i ekspertgruppens arbejde. Hver især indgav de støttende udsagn og erkendte, at der var behov at løse en række bredere problemer vedrørende de grundlæggende rettigheder og databeskyttelse for at komme videre. Repræsentanter for sekretariatet for Europa-Parlamentets udvalg om borgernes rettigheder og retlige og indre anliggender og Rådets generalsekretariat deltog som observatører. Ekspertgruppen på højt niveau konkluderede, at det er **nødvendigt og teknisk gennemførligt at arbejde hen imod praktiske interoperabilitetsløsninger**, og at de i princippet både kan sikre operationelle gevinster og indføres under overholdelse af kravene om databeskyttelse.

Med udgangspunkt i ekspertgruppens rapport og henstillinger fremlagde Kommissionen i den *syvende statusrapport om gennemførelsen af en effektiv og ægte sikkerhedsunion*[9] en **ny tilgang til forvaltningen af data** vedrørende grænser, sikkerhed og migrationsforvaltning, hvor alle centrale EU-informationssystemer for sikkerhed, grænse- og migrationsforvaltning er interoperable under fuld overholdelse af de grundlæggende rettigheder. Kommissionen meddelte, at den agter at fortsætte bestræbelserne for at skabe en europæisk søgeportal, der gør det muligt at foretage søgninger samtidigt i alle relevante EU-systemer på områderne sikkerhed, grænse- og migrationsforvaltning, eventuelt med mere strømlinede regler for adgang med henblik på retshåndhævelse, og at udvikle en fælles biometrisk matchtjeneste til

---

4 Europa-Parlamentets beslutning af 6. juli 2016 om de strategiske prioriteringer for Kommissionens arbejdsprogram for 2017 2016/2773(RSP).

5 Unionens tilstand 2016 (14.9.2016): https://ec.europa.eu/commission/state-union-2016_da.

6 Det Europæiske Råds konklusioner (15.12.2016): http://www.consilium.europa.eu/da/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

7 Kommissionens afgørelse af 17. juni 2016 om nedsættelse af en ekspertgruppe på højt niveau vedrørende informationssystemer og interoperabilitet – 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

disse systemer (eventuelt med hit/intet hit-påtegninger[10]) og et fælles identitetsregister. Den meddelte, at den snarest muligt ville fremlægge et lovforslag om interoperabilitet.

Det Europæiske Råd gentog i sine konklusioner fra juni 2017[11], at det var nødvendigt at handle. Med udgangspunkt i Rådets (retlige og indre anliggende) konklusioner fra juni 2017[12] opfordrede Det Europæiske Råd Kommissionen til hurtigst muligt at udarbejde udkast til lovgivning til vedtagelse af de forslag, som er fremsat af ekspertgruppen på højt niveau. Dette initiativ imødekommer også Rådets opfordring til at indføre en omfattende ramme for retshåndhævende myndigheders adgang til de forskellige databaser inden for retlige og indre anliggender med henblik på større forenkling, konsekvens, effektivitet og opmærksomhed over for operationelle behov[13]. For at styrke bestræbelserne på at gøre EU til et mere sikkert samfund, i fuld overensstemmelse med de grundlæggende rettigheder, fremlagde Kommissionen i forbindelse med sit 2018-arbejdsprogram[14] et forslag om interoperabilitet mellem informationssystemer, der skal fremlægges ved udgangen af 2017.

- **Forslagets formål**

De generelle målsætninger for dette initiativ følger af de traktatfæstede mål om forbedring af forvaltningen af de ydre Schengengrænser og bidrag til den indre sikkerhed i den Europæiske Union. De er også en følge af politiske beslutninger truffet af Kommissionen og af Rådets/Det Europæiske Råds relevante konklusioner. Disse målsætninger er yderligere uddybet i den europæiske dagsorden for migration og efterfølgende meddelelser, herunder meddelelsen om bevarelse og styrkelse af Schengenområdet[15], den europæiske dagsorden om sikkerhed[16] og Kommissionens arbejds- og statusrapporter om at bane vejen for en effektiv og ægte sikkerhedsunion[17].

Målene i dette forslag bygger især på meddelelsen fra april 2016 og resultaterne fra ekspertgruppen på højt niveau, og målsætningerne i dette forslag er derfor uløseligt knyttet til ovenstående.

Dette forslags specifikke mål er at:

1) sikre, at slutbrugerne, navnlig grænsevagter, retshåndhævende myndigheder, immigrationsmyndigheder og retlige myndigheder, får **hurtig, problemfri, systematisk og kontrolleret adgang** til de oplysninger, som de behøver for at varetage deres opgaver

[10] Nyt koncept for indbygget privatlivsbeskyttelse ("privacy-by-design"), der begrænser adgangen til alle data ved at begrænse denne til en hit/intet hit-påtegning, der angiver, om der findes (eller ikke findes samme) data.
[11] Det Europæiske Råds konklusioner, 22.-23. juni 2017.
[12] Resultatet af det 3546. møde i Rådet om Retlige og Indre Anliggender den 8. og 9. juni 2017, 10136/17.
[13] Efter at Rådets Faste Repræsentanters Komité (Coreper) havde givet Rådets formandskab mandat til at indlede interinstitutionelle forhandlinger om EU's ind- og udrejsesystem den 2. marts 2017, enedes man om et udkast til Rådets erklæring, hvori Kommissionen blev opfordret til at foreslå en omfattende ramme for de retshåndhævende myndigheders adgang til de forskellige databaser inden for retlige og indre anliggender med henblik på større forenkling, sammenhæng, effektivitet og opmærksomhed på operationelle behov (kortfattet referat 7177/17, 21.3.2017).
[14] COM(2017) 650 final.
[15] COM(2017) 570 final.
[16] COM(2015) 185 final.
[17] COM(2016) 230 final.

2) levere en løsning, der gør det muligt at **påvise, at flere identiteter** er knyttet til det samme sæt biometriske data med det dobbelte formål at sikre korrekt identificering af personer i god tro og **bekæmpe identitetssvig**

3) lette politimyndighedernes **identitetskontrol af tredjelandsstatsborgere** på en medlemsstats område og

4) lette og **effektivisere retshåndhævende myndigheders adgang** til informationssystemer, som ikke vedrører retshåndhævelse, på EU-niveau, hvis det er nødvendigt for at forebygge, efterforske, opdage eller retsforfølge alvorlige strafbare handlinger og terrorisme.

Ud over disse primære operationelle mål vil dette forslag også bidrage til:

- at lette den tekniske og operationelle **gennemførelse i medlemsstaterne** af eksisterende og fremtidige nye informationssystemer
- at styrke og effektivisere den **datasikkerhed og databeskyttelse**, der gælder for de respektive systemer og
- forbedre og harmonisere kravene til **datakvaliteten** i de respektive systemer.

Endelig omfatter dette forslag bestemmelser om oprettelse og styring af det universelle meddelelsesformat (UMF) som EU-standard for udvikling af informationssystemer inden for retlige og indre anliggender og oprettelse af et centralt opbevaringssted for rapportering og statistik.

- **Forslagets anvendelsesområde**

Sammen med det tilknyttede forslag, som blev forelagt samme dag, fokuserer dette forslag om interoperabilitet på de EU-informationssystemer vedrørende sikkerhed, grænse- og migrationsforvaltning, der drives på centralt plan, hvoraf de tre allerede findes, ét er ved at blive udviklet, og forslagene til de to andre er ved at blive drøftet mellem Europa-Parlamentet og Rådet. Hvert system har sine egne målsætninger, formål, retsgrundlag, regler, brugergrupper og institutionelle kontekst.

De tre hidtil eksisterende centrale informationssystemer er:

- **Schengeninformationssystemet (SIS)** med et bredt spektrum af indberetninger om personer (nægtelse af indrejse eller afslag på ansøgning om opholdstilladelse, en europæisk arrestordre, forsvundne personer, bistand i forbindelse med retssager, diskret og målrettet kontrol) og genstande (herunder bortkomne, stjålne og ugyldiggjorte identitets- eller rejsedokumenter)[18].
- **Eurodac**-systemet med fingeraftryksoplysninger om asylansøgere og tredjelandsstatsborgere, der har krydset de ydre grænser ulovligt, eller som opholder sig ulovligt i en medlemsstat, og
- **visuminformationssystemet** (VIS) med data om visa til kortvarigt ophold.

[18] Kommissionens foreslår i sit udkast til forordning om SIS fra december 2016 at udvide dette til også at omfatte afgørelser om tilbagesendelse og undersøgelseskontrol.

Foruden disse eksisterende systemer foreslog Kommissionen i 2016-2017 tre nye centrale europæiske informationssystemer:

- **ind- og udrejsesystemet**, hvis retsgrundlag netop er blevet vedtaget, og som skal erstatte det nuværende system med manuel stempling af pas, og som elektronisk registrerer navn, type af rejsedokument og biometriske identifikatorer samt dato og sted for ind- og udrejse for tredjelandsstatsborgere, der besøger Schengenområdet med henblik på et kortvarigt ophold
- det foreslåede **EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS)**, som, når det er vedtaget, vil være et stort set automatiseret system, der indsamler og verificerer de oplysninger, der indgives af tredjelandsstatsborgere, der er fritaget for visumpligten, forud for deres rejse til Schengenområdet og
- det foreslåede **europæiske informationssystem til udveksling af oplysninger fra strafferegistre vedrørende tredjelandsstatsborgere (ECRIS-TCN-systemet**), som er et elektronisk system til udveksling af oplysninger om tidligere domme afsagt af straffedomstole over tredjelandsstatsborgere i EU.

Disse seks systemer supplerer hinanden og fokuserer – med undtagelse af Schengeninformationssystemet (SIS) – udelukkende på tredjelandsstatsborgere. Systemerne støtter de nationale myndigheder i forvaltningen af grænser, migration, visumbehandling og asyl og bekæmpelse af kriminalitet og terrorisme. Sidstnævnte er navnlig tilfældet i forhold til SIS, som er det mest udbredte informationsudvekslingsinstrument med henblik på retshåndhævelse i dag.

Ud over disse informationssystemer, som styres centralt i EU, omfatter forslaget også **Interpols** database over stjålne og bortkomne rejsedokumenter (SLTD), som i henhold til bestemmelserne i Schengengrænsekodeksen bruges systematisk ved EU's ydre grænser, og Interpols database over rejsedokumenter med tilknyttede notifikationer (TDAWN). Det dækker også data fra **Europol**, så vidt det er relevant for driften af det foreslåede ETIAS-system og med henblik på at bistå medlemsstaterne, når de søger oplysninger om grov kriminalitet og terrorisme.

Nationale informationssystemer og decentrale EU-informationssystemer er ikke omfattet af dette initiativ. Forudsat at der påvises et behov, kan decentrale systemer som dem, der fungerer på grundlag af Prüm-rammen[19], direktivet om passagerlister[20] og direktivet om forhåndsinformation om passagerer[21] på et senere tidspunkt blive knyttet til en eller flere af de komponenter, der foreslås under dette initiativ[22].

For at tage højde for sondringen mellem forhold, der udgør en udvikling af Schengenreglerne om grænser og visum på den ene side, og andre systemer, der vedrører Schengenreglerne om politisamarbejde eller ikke er knyttet til Schengenreglerne på den anden, vedrører dette forslag adgangen til visuminformationssystemet, Schengeninformationssystemet, som i

[19] http://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.
[20] http://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1508936384641&uri=CELEX:32016L06 81.
[21] Rådets direktiv 2004/82/EF af 29. april 2004 om transportvirksomheders forpligtelse til at fremsende oplysninger om passagerer.
[22] For så vidt angår toldsystemer opfordrede Rådet i sine konklusioner fra juni 2017 på samme måde Kommissionen til at gennemføre en gennemførlighedsundersøgelse for yderligere at udforske de tekniske, operationelle og retlige aspekter ved sikkerheds- og grænseforvaltningssystemernes interoperabilitet med toldsystemerne og forelægge sine resultater for Rådet med henblik på drøftelse heraf senest inden udgangen af 2018.

øjeblikket er reguleret ved forordning (EF) nr. 1987/2006, ind- og udrejsesystemet og det europæiske system vedrørende rejseoplysninger og rejsetilladelser.

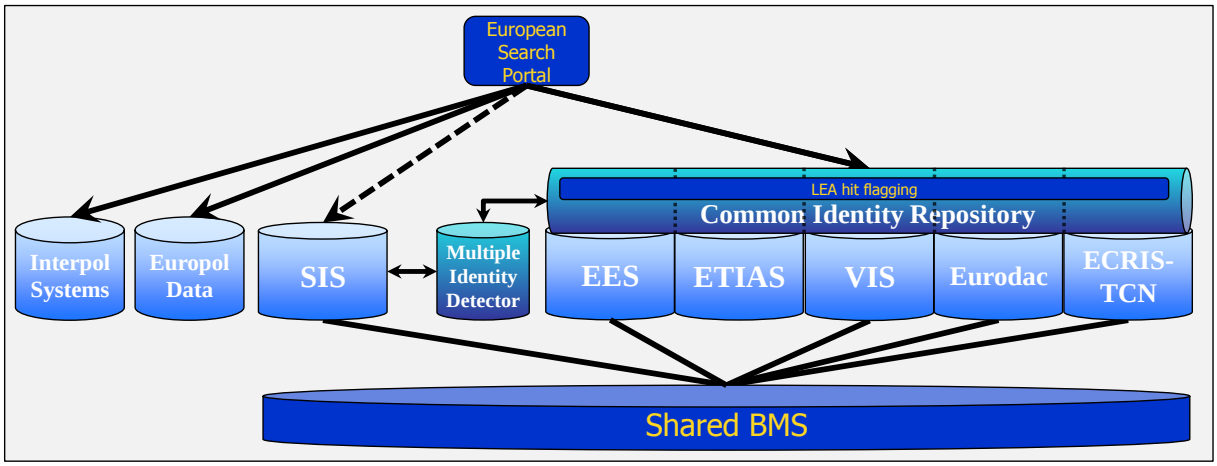
- **De nødvendige tekniske komponenter med henblik på at opnå interoperabilitet**

For at nå målene i dette forslag skal der fastsættes fire komponenter til funktionskompatibilitet:

- En europæisk søgeportal – ESP
- En fælles biometrisk matchtjeneste – fælles BMS
- Et fælles identitetsregister
- En multiidentitetsdetektor – MID

Hver af disse komponenter er beskrevet i detaljer i Kommissionens arbejdsdokument om den konsekvensanalyse, der ledsager dette forslag.

De fire komponenter fører sammen til følgende interoperabilitetsløsning:



Disse fire komponenters mål og funktion kan sammenfattes som følger:

1) Den **europæiske søgeportal (ESP)** er den komponent, som gør det muligt at foretage søgninger i flere systemer (centralt SIS, Eurodac, VIS, det kommende ind- og udrejsesystem og det foreslåede ETIAS- og ECRIS-TCN-system samt de relevante Interpol-systemer og Europol-data) ved hjælp af identitetsdata (både biografiske og biometriske). Det vil sikre, at brugere af EU-informationssystemerne har hurtig, problemfri, effektiv, systematisk og kontrolleret adgang til alle de oplysninger, de skal bruge for at udføre deres opgaver.

   En forespørgsel gennem den europæiske søgeportal vil straks, på få sekunder, give oplysninger fra de forskellige systemer, som brugeren har lovlig adgang til. Afhængigt af formålet med forespørgslen og de tilsvarende adgangsrettigheder vil ESP være forsynet med specifikke konfigurationer.

   ESP behandler ikke alle nye data, og den lagrer heller ikke nogen data. Den fungerer som en one-stop-shop eller en "meddelelsesformidler", der søger i forskellige centrale systemer og indhenter de nødvendige oplysninger helt problemfrit og i fuld

overensstemmelse med kravene til adgangskontrol og databeskyttelse i de underliggende systemer. ESP letter korrekt og autoriseret brug af hvert af de eksisterende EU-informationssystemer og vil gøre det nemmere og billigere for medlemsstaterne at konsultere og bruge systemerne i overensstemmelse med de retlige instrumenter, der regulerer disse systemer.

2) Den **fælles biometriske matchtjeneste (fælles BMS)** vil gøre det muligt at søge efter og sammenligne biometriske oplysninger (fingeraftryk og ansigtsbilleder) fra flere centrale systemer (navnlig SIS, Eurodac, VIS, det fremtidige ind- og udrejsesystem og det foreslåede ECRIS-TCN-system). Det foreslåede ETIAS-system kommer ikke til at indeholde biometriske data og vil derfor ikke være knyttet til den fælles BMS.

   Hvis de eksisterende centrale systemer (SIS, Eurodac, VIS) i øjeblikket har en særlig proprietær søgemaskine til biometriske data[23], vil en delt biometrisk matchtjeneste skabe en fælles platform, hvor der på samme tid søges efter og sammenlignes data. Den fælles BMS vil give betydelige fordele med hensyn til sikkerhed, omkostninger, vedligeholdelse og drift ved at benytte én unik teknologisk komponent i stedet for fem forskellige. De biometriske data (fingeraftryk og ansigtsbilleder) opbevares udelukkende i de underliggende systemer. Den fælles BMS opretter og gemmer en matematisk gengivelse af de biometriske prøver (en skabelon), men kasserer de faktiske data, som dermed kun lagres ét sted og kun én gang.

   Den fælles BMS vil være en nøglefaktor i forhold til at opdage forbindelser mellem datasættene og forskellige identiteter antaget af den samme person i forskellige centrale systemer. Uden en fælles BMS vil ingen af de andre tre komponenter kunne fungere.

3) Det **fælles identitetsregister** vil være den fælles komponent til lagring af biografiske[24] og biometriske identitetsdata for tredjelandsstatsborgere registreret i Eurodac, VIS, det fremtidige ind- og udrejsesystem, det foreslåede ETIAS-system og det foreslåede ECRIS-TCN-system. Hvert af disse fem centrale systemer registrerer eller vil registrere biografiske data om bestemte personer af særlige grunde. Dette ændres ikke. De relevante identitetsdata vil blive gemt i det fælles identitetsregister, men vil fortsat "høre til" i de respektive underliggende systemer, der registrerede disse data.

   Det fælles identitetsregister vil ikke indeholde SIS-data. Den komplekse tekniske struktur i SIS, der indeholder nationale kopier, delvise nationale kopier og eventuelle nationale biometriske matchsystemer, vil gøre det fælles identitetsregister meget komplekst i en grad, hvor det ikke længere er teknisk og økonomisk gennemførligt.

   Det centrale mål for det fælles identitetsregister er at lette den biografiske identifikation af en tredjelandsstatsborger. Det vil medføre hurtigere drift, øget effektivitet og stordriftsfordele. Oprettelsen af det fælles identitetsregister er nødvendigt for at muliggøre en effektiv identitetskontrol af tredjelandsstatsborgere, herunder på en medlemsstats område. Ved derudover at føje funktionen med hit/intet hit-påtegninger til det fælles identitetsregister vil det være muligt at kontrollere, om der findes (eller ikke findes) data i de systemer, der er omfattet af det fælles identitetsregister gennem en

[23] Disse biometriske søgemaskiner er teknisk benævnt elektroniske fingeraftryksidentifikationssystemer (AFIS) eller elektroniske biometriske identifikationssystemer (ABIS).

[24] Biografiske data, der kan findes i rejsedokumentet, omfatter: efternavn, fornavn, køn, fødselsdato, rejsedokumentnummer. De omfatter ikke adresser, tidligere navne, biometriske data osv.

simpel hit/intet hit-påtegning. På denne måde vil det fælles identitetsregister også hjælpe med at effektivisere de retshåndhævende myndigheders adgang til informationssystemer, som ikke vedrører retshåndhævelse, og samtidig opretholde en høj databeskyttelse (se afsnittet om totrinstilgangen til de retshåndhævende myndigheders adgang nedenfor).

Ud af de fem systemer, som er omfattet af det fælles identitetsregister, er det fremtidige ind- og udrejsesystem, det foreslåede ETIAS-system og det foreslåede ECRIS-TCN-system nye systemer, der stadig skal udvikles. Det nuværende Eurodac har ikke biografiske data. Den del vil blive udviklet, når det nye retsgrundlag for Eurodac er vedtaget. Det nuværende VIS indeholder biografiske data, men det nødvendige samspil mellem VIS og det fremtidige ind- og udrejsesystem kræver en opgradering af det eksisterende VIS. Oprettelsen af det fælles identitetsregister vil derfor ske på det helt rigtige tidspunkt. Det ville ikke på nogen måde indebære en fordobling af de eksisterende data. Teknisk set vil det fælles identitetsregister blive udviklet på grundlag af platformen for ind- og udrejsesystemet/ETIAS.

4) **Multiidentitetsdetektoren (MID)** kontrollerer, om de identitetsdata, der søges, findes i mere end ét af de systemer, det er tilknyttet. MID dækker de systemer, der gemmer identitetsdata i det fælles identitetsregister (Eurodac, VIS, det fremtidige ind- og udrejsesystem, det foreslåede ETIAS og det foreslåede ECRIS-TCN-system) samt SIS. MID vil gøre det muligt at påvise flere identiteter knyttet til det samme sæt af biometriske data, med det dobbelte formål at sikre en korrekt identifikation af personer i god tro og bekæmpe identitetstyveri.

MID vil gøre det muligt at fastslå, at forskellige navne tilhører samme identitet. Det er en nødvendig fornyelse at kunne bekæmpe svigagtig anvendelse af identiteter, hvilket er et alvorligt brud på sikkerheden. MID vil kun vise de biografiske identitetsdata, som har et link i forskellige centrale systemer. Disse links vil blive opdaget ved hjælp af en fælles biometrisk matchtjeneste og vil skulle bekræftes eller afvises af den myndighed, der har registreret oplysningerne i det system, som førte til oprettelsen af linket. For at kunne bistå autoriserede brugere af MID med denne opgave vil systemet skulle markere de identificerede links i fire kategorier:

- Gult – potentielt forskellige biografiske identiteter på én og samme person
- Hvidt – bekræftelse af, at forskellige biografiske identiteter tilhører samme person i god tro
- Grønt – bekræftelse af, at forskellige personer i god tro tilfældigvis har samme biografiske identitet
- Rødt – mistanke om, at forskellige biografiske identiteter anvendes ulovligt af den samme person.

Dette forslag beskriver de procedurer, som skal indføres til at håndtere disse forskellige kategorier. Enhver tvivl om identiteten på de berørte personer i god tro bør så hurtigt som muligt fjernes ved at gøre det gule link til et bekræftet grønt eller hvidt link, således at der ikke opstår unødvendige gener. Hvis vurderingen på den anden side fører til bekræftelse af et rødt link eller en ændring fra gult til rødt link, skal der træffes passende foranstaltninger.

- **Totrinstilgangen for de retshåndhævende myndigheders adgang til det fælles identitetsregister**

Retshåndhævelse er defineret som et sekundært eller underordnet mål i Eurodac, VIS, det fremtidige ind- og udrejsesystem og det foreslåede ETIAS-system. Muligheden for at få adgang til data lagret i disse systemer med henblik på retshåndhævelse er derfor begrænset. Retshåndhævende myndigheder kan kun søge direkte i disse informationssystemer, som ikke vedrører retshåndhævelse, med henblik på forebyggelse, efterforskning, opdagelse eller retsforfølgning af terrorisme og andre alvorlige strafbare handlinger. Desuden er de respektive systemer underlagt forskellige adgangsbetingelser og garantier, og nogle af de nuværende regler kunne sænke hastigheden af myndighedernes legitime brug af systemerne. Mere generelt begrænser princippet om forudgående søgebegrænsninger muligheden for, at medlemsstaternes myndigheder kan benytte systemerne til berettigede retshåndhævelsesformål, hvilket kan betyde, at muligheden for at finde frem til de nødvendige oplysninger, går tabt.

I sin meddelelse fra april 2016 erkendte Kommissionen, at der var behov for at optimere de eksisterende værktøjer til retshåndhævelsesformål under hensyntagen til kravene til databeskyttelse. Dette behov blev bekræftet og gentaget af medlemsstaterne og relevante agenturer inden for rammerne af ekspertgruppen på højt niveau.

På baggrund af ovenstående giver dette forslag, hvorved der oprettes et fælles identitetsregister med en funktionalitet med hit/intet hit-påtegninger, mulighed for at få adgang til ind- og udrejsesystemet, VIS, ETIAS og Eurodac ved hjælp af en **totrinstilgang til datakonsultation**. Denne totrinstilgang ændrer ikke ved, at retshåndhævelse er et strengt accessorisk mål for disse systemer, og at der derfor skal følges en række strenge adgangsregler.

I første omgang vil en retshåndhævende myndighed foretage en søgning på en bestemt person ved hjælp af personens identitetsdata, rejsedokument eller biometriske data for at kontrollere, om der er lagret oplysninger om den person, der søges efter, i det fælles identitetsregister. Såfremt der findes sådanne data, vil den retshåndhævende myndighed modtage **et svar med angivelse af, hvilke(t) EU-informationssystem(er) der indeholder data** om denne person (**hit-påtegning**). Den retshåndhævende myndighed vil ikke have reel adgang til data i alle de underliggende systemer.

Dernæst kan den retshåndhævende myndighed anmode om adgang til de systemer, der er blevet angivet som indeholdende data, for at opnå et fuldstændigt dossier om den person, der søges oplysninger om, **i overensstemmelse med de gældende regler og procedurer, der er fastsat for de enkelte systemer**. Adgangen på dette næste trin vil fortsat afhænge af, at en udpeget myndighed har givet en forhåndsgodkendelse heraf, og vil fortsat kræve et bestemt bruger-id og logføring.

Denne nye tilgang vil også give de retshåndhævende myndigheder en merværdi på grund af **de potentielle links** i MID. MID understøtter det fælles identitetsregister med henblik på at finde eksisterende links, hvilket gør søgningen endnu mere præcis. MID vil være i stand til at angive, om personen er **kendt under forskellige identiteter** i forskellige informationssystemer.

Datakonsultationen i to trin er særlig værdifuld i de tilfælde, hvor den mistænkte, gerningsmanden eller det formodede offer for en terrorhandling eller andre alvorlige forbrydelser **er ukendt**. I disse tilfælde vil det fælles identitetsregister faktisk gøre det muligt at indkredse det informationssystem, der indeholder oplysninger om personen, i en enkelt søgning. Herved bliver de eksisterende betingelser for de tidligere søgninger i nationale databaser og for en tidligere søgning i det elektroniske fingeraftryksidentifikationssystem i andre medlemsstater i henhold til afgørelse 2008/615/RIA ("Prüm-kontrol") overflødige.

Den nye totrinstilgang for søgninger vil **først træde i kraft**, når de nødvendige **interoperabilitetskomponenter er fuldt operationelle**.

- **Yderligere elementer i dette forslag til støtte for interoperabilitetskomponenterne**

1) Ud over ovenstående komponenter indeholder dette forslag til forordning også et forslag om at etablere et **centralt register til rapportering og statistik (CRRS)**. Dette register er nødvendigt for at muliggøre oprettelse og deling af rapporter med (anonyme) statistiske data til politiske, operationelle og datakvalitetsmæssige formål. Den nuværende praksis med kun at indsamle statistiske data om de enkelte informationssystemer er til skade for datasikkerheden og ydeevnen og gør det ikke muligt at forbinde data på tværs af systemer.

   CRRS vil være et særligt og særskilt register for anonyme statistiske oplysninger hentet i SIS, VIS, Eurodac, det fremtidige ind- og udrejsesystem, det foreslåede ETIAS-system, ECRIS-TCN-systemet, det fælles identitetsregister, multiidentitetsdetektoren og den fælles biometriske matchtjeneste. Registret vil give mulighed for en sikker udveksling af rapporter (som reguleret af de respektive retsakter) med medlemsstaterne, Kommissionen (herunder Eurostat) og EU-agenturer.

   Oprettelsen af et centralt register i stedet for særskilte registre for de enkelte systemer vil føre til lavere omkostninger og mindre arbejde til etablering, drift og vedligeholdelse. Det vil også medføre en højere grad af datasikkerhed, da dataene lagres, og adgangskontrollen forvaltes i ét register.

2) I dette forslag til forordning foreslås det også at fastsætte det **universelle meddelelsesformat (UMF)** som den standard, der skal anvendes på EU-plan med henblik på at samordne interaktioner mellem flere systemer på en måde, der sikrer interoperabilitet, herunder de systemer, som er udviklet og forvaltes af eu-LISA. Europol og Interpol vil også blive opfordret til at anvende denne standard.

   Med UMF-standarden introduceres et fælles og ensartet teknisk sprog til at beskrive og sammenkæde dataelementer, især elementer vedrørende personer og (rejse)dokumenter. Brugen af UMF til udvikling af nye informationssystemer sikrer en enklere integration og interoperabilitet med andre systemer, navnlig i medlemsstater, der har behov for at udvikle grænseflader til at kommunikere med disse nye systemer. I denne forbindelse kan det overvejes at indføre obligatorisk anvendelse af UMF ved udvikling af nye systemer som en nødvendig forudsætning for indførelsen af interoperabilitetskomponenter i denne forordning.

For at sikre at UMF-standarden udrulles fuldstændigt i hele EU, foreslås en passende forvaltningsstruktur. Kommissionen vil være ansvarlig for at etablere og udvikle UMF-standarden inden for rammerne af en undersøgelsesprocedure med medlemsstaterne. Associerede Schengenlande, EU-agenturer og internationale organisationer, der deltager i UMF-projekter (som f.eks. eu-LISA, Europol og Interpol), vil også blive inddraget. Den foreslåede forvaltningsstruktur er afgørende for UMF i forhold til at forlænge og udvide standarden og samtidig sikre maksimal brugervenlighed og anvendelighed.

3) Dette forslag til forordning indfører desuden begreberne **elektroniske datakvalitetskontrolmekanismer** og fælles kvalitetsindikatorer samt medlemsstaternes behov for at sikre den højeste grad af datakvalitet, når de indlæser data i og anvender systemerne. Hvis dataene ikke er af den højeste kvalitet, kan det få konsekvenser, ikke blot med hensyn til muligheden for at identificere efterlyste personer, men også ved at påvirke uskyldige menneskers grundlæggende rettigheder. For at overvinde de problemer, der kan opstå, når menneskelige operatører indlæser oplysninger, kan automatiske valideringsregler forhindre operatørerne i at begå fejl. Målet er at finde tilsyneladende forkerte eller inkonsekvente data automatisk, så den oprindelige medlemsstat er i stand til at verificere dataene og eventuelt træffe de fornødne afhjælpende foranstaltninger. Dette vil blive suppleret med regelmæssige datakvalitetsrapporter udarbejdet af eu-LISA.

- **Følger for andre juridiske instrumenter**

Sammen med det tilknyttede forslag indfører dette forslag til forordning nyskabelser, der vil kræve ændringer af andre retsakter:

- Forordning (EU) 2016/399 (Schengengrænsekodeksen)
- Forordning (EU) 2017/2226 (forordningen om ind- og udrejsesystemet)
- Forordning (EF) nr. 767/2008 (VIS-forordningen)
- Rådets afgørelse 2004/512/ EF (VIS-afgørelsen)
- Rådets afgørelse 2008/633/RIA (afgørelsen om VIS/adgang for retshåndhævende myndigheder)
- [ETIAS-forordningen]
- [Eurodac-forordningen]
- [SIS-forordningerne]
- [ECRIS-TCN-forordningen, herunder de tilsvarende bestemmelser i forordning (EU) 2016/1624 (forordningen om den europæiske grænse- og kystvagt)]
- [eu-LISA-forordningen]

Det nuværende forslag og det tilknyttede forslag indeholder nærmere bestemmelser om de nødvendige ændringer af de retlige instrumenter, der for øjeblikket er stabile tekster som vedtaget af Europa-Parlamentet og Rådet: Schengengrænsekodeksen, forordningen om ind- og udrejsesystemet, VIS-forordningen, Rådets afgørelse 2008/633/RIA og Rådets afgørelse 2004/512/EF.

De øvrige nævnte instrumenter (forordningerne om ETIAS, Eurodac, SIS, ECRIS-TCN, eu-LISA) er i øjeblikket genstand for forhandlinger i Europa-Parlamentet og Rådet. For disse instrumenter er det derfor ikke muligt at fastlægge de nødvendige ændringer på dette trin.

Kommissionen forelægger sådanne ændringer for hvert af disse instrumenter, senest to uger efter der er indgået en politisk aftale om de respektive udkast til forordninger.

- **Sammenhæng med de gældende regler på samme område**

Dette forslag falder ind under rammerne for den mere generelle proces, der blev lanceret i meddelelsen fra april 2016 om stærkere og mere intelligente informationssystemer for grænser og sikkerhed, og det efterfølgende arbejde i ekspertgruppen på højt niveau om informationssystemer og interoperabilitet. Formålet er at forfølge tre mål:

a) styrke og maksimere fordelene ved de **eksisterende informationssystemer**

b) løse problemet med manglende oplysninger ved at oprette nye informationssystemer

c) fremme interoperabilitet mellem disse systemer.

Med hensyn til det første mål vedtog Kommissionen i december 2016 forslag om en yderligere styrkelse af det nuværende Schengeninformationssystem (SIS)[25]. Med hensyn til Eurodac blev forhandlingerne om det reviderede retsgrundlag efter Kommissionens forslag fra maj 2016[26] fremskyndet. Et forslag til et nyt retsgrundlag for visuminformationssystemet (VIS) er også under udarbejdelse og vil blive forelagt i andet kvartal af 2018.

Med hensyn til det andet mål blev forhandlingerne om Kommissionens forslag fra april 2016 om oprettelse af et ind- og udrejsesystem[27] afsluttet allerede i juli 2017, da Europa-Parlamentet og Rådet nåede frem til en politisk aftale, som blev bekræftet af Europa-Parlamentet i oktober 2017 og formelt vedtaget af Rådet i november 2017. Retsgrundlaget træder i kraft i december 2017. Forhandlingerne om forslaget fra november 2016 om oprettelse af et EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS)[28] er indledt og ventes at blive afsluttet i de kommende måneder. I juni 2017 foreslog Kommissionen et retsgrundlag for at afhjælpe problemet med andre manglende oplysninger: det europæiske informationssystem til udveksling af oplysninger fra strafferegistre vedrørende tredjelandsstatsborgere (ECRIS-TCN-systemet)[29]. Her har Europa-Parlamentet og Rådet igen tilkendegivet, at de sigter mod en snarlig vedtagelse af dette retsgrundlag.

Nærværende forslag vedrører det tredje mål, som er angivet i meddelelsen fra april 2016.

- **Sammenhæng med Unionens politik på området retlige og indre anliggender**

Dette forslag opfylder og er sammen med det tilknyttede forslag i overensstemmelse med den europæiske dagsorden for migration og efterfølgende meddelelser, herunder meddelelsen om bevarelse og styrkelse af Schengenområdet[30], samt den europæiske dagsorden om sikkerhed[31]

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.
[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.

og Kommissionens arbejde og statusrapporter om indførelsen af en effektiv og ægte sikkerhedsunion[32]. Det er i overensstemmelse med andre EU-politikker, navnlig følgende:

- Intern sikkerhed: I den europæiske dagsorden om sikkerhed anføres det, at fælles høje standarder for grænseforvaltning er afgørende for at undgå grænseoverskridende kriminalitet og terrorisme. Dette forslag bidrager yderligere til at opnå en høj grad af intern sikkerhed ved at tilbyde myndighederne hjælp til at få hurtig, sammenhængende, systematisk og kontrolleret adgang til de oplysninger, de har brug for.
- Asyl: Forslaget omfatter Eurodac som et af EU's centrale systemer, der skal være omfattet af interoperabilitet.
- Ekstern grænseforvaltning og sikkerhed: Dette forslag styrker SIS- og VIS-systemet, der bidrager til en effektiv kontrol af EU's ydre grænser, samt det fremtidige ind- og udrejsesystem og det foreslåede ETIAS-system og ECRIS-TCN-systemet.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

• Retsgrundlag

Det vigtigste retsgrundlag vil være følgende artikler i traktaten om Den Europæiske Unions funktionsmåde: Artikel 16, stk. 2, artikel 74, artikel 77, stk. 2, litra a), b), d) og e).

I henhold til artikel 16, stk. 2, er Unionen bemyndiget til at vedtage foranstaltninger vedrørende beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger foretaget af Unionens institutioner, organer og agenturer samt af medlemsstaterne under udøvelse af aktiviteter, der er omfattet af EU-retten, og regler for den frie udveksling af personoplysninger. I henhold til artikel 74 kan Rådet vedtage foranstaltninger med henblik på at sikre administrativt samarbejde mellem de kompetente myndigheder i medlemsstaterne inden for området med retfærdighed, frihed og sikkerhed. I henhold til artikel 77, stk. 2, litra a), b), d) og e), kan Europa-Parlamentet og Rådet træffe foranstaltninger vedrørende den fælles visumpolitik og andre tilladelser til kortvarigt ophold, personkontrol ved passage af de ydre grænser, nødvendige tiltag til den gradvise udvikling af et integreret system for forvaltningen af de ydre grænser og reglerne om, at personer uanset nationalitet ikke kontrolleres ved passage af de indre grænser.

• Nærhedsprincippet

Fri bevægelighed inden for EU kræver, at EU's ydre grænser forvaltes effektivt for at garantere sikkerheden. Medlemsstaterne har derfor aftalt at tage disse udfordringer op i fællesskab, især via udveksling af oplysninger gennem centraliserede systemer i EU på området retlige og indre anliggender. Dette bekræftes af de forskellige konklusioner, som er vedtaget af Det Europæiske Råd og Rådet, især siden 2015.

Fraværet af kontrol ved de indre grænser kræver en forsvarlig forvaltning af Schengenområdets ydre grænser, hvor hver medlemsstat eller det associerede Schengenland skal kontrollere de ydre grænser på vegne af de øvrige Schengenstater. Følgelig kan ingen medlemsstat alene håndtere irregulær migration og grænseoverskridende kriminalitet. Tredjelandsstatsborgere, der kommer ind i området uden kontrol ved de indre grænser, kan

[32] COM(2016) 230 final.

rejse frit inden for området. I et område uden indre grænser bør der træffes fælles foranstaltninger mod ulovlig indvandring og international kriminalitet og terrorisme, herunder gennem påvisning af identitetstyveri, og sådanne foranstaltninger lykkes kun, hvis de håndteres på EU-niveau.

Der er indført eller ved at blive indført vigtige fælles informationssystemer på EU-plan. For at forbedre interoperabiliteten mellem disse informationssystemer kræves det nødvendigvis, at der træffes foranstaltninger på EU-plan. Kernen i forslaget er, at effektiviteten og anvendelsen af de centraliserede systemer, der forvaltes af eu-LISA, skal forbedres. På grund af omfanget og virkningerne af de planlagte tiltag kan de grundlæggende mål kun opfyldes effektivt og systematisk på EU-plan.

- **Proportionalitet**

Som forklaret fuldt ud i den konsekvensanalyse, der ledsager dette forslag til forordning, anses de politiske valg i forslaget for at være i overensstemmelse med proportionalitetsprincippet. De går ikke ud over, hvad der er nødvendigt for at nå de ønskede mål.

Den **europæiske søgeportal (ESP)** er et nødvendigt redskab til at styrke den autoriserede brug af de eksisterende og fremtidige EU-informationssystemer. Virkningen af ESP med hensyn til databehandling er meget begrænset. Den lagrer ikke data, undtagen informationer om de forskellige brugerprofiler i ESP og de data- og informationssystemer, som de har adgang til, og holder styr på deres anvendelse ved hjælp af logfiler. ESP's rolle som en grænseflade, der muliggør og letter en effektiv informationsudveksling, er forholdsmæssig, nødvendig og begrænset, hvad angår søgninger og adgangsrettigheder i henhold til retsgrundlagene for informationssystemerne og den foreslåede forordning om interoperabilitet.

Den **fælles biometriske matchtjeneste (fælles BMS)** er nødvendig for driften af ESP, det fælles identitetsregister og multiidentitetsdetektoren, ligesom den letter brug og vedligeholdelse af de eksisterende og fremtidige relevante EU-informationssystemer. Dens funktioner gør det muligt at foretage søgninger efter biometriske data fra forskellige kilder på en effektiv, problemfri og systematisk måde. De biometriske data lagres og opbevares af de underliggende systemer. Den fælles BMS opretter skabeloner, men kasserer de faktiske billeder. Dataene lagres således kun ét sted og kun én gang.

Det fælles identitetsregister er nødvendigt for at opfylde målet om en korrekt identifikation af tredjelandsstatsborgere, f.eks. under en identitetskontrol inden for Schengenområdet. Det fælles identitetsregister understøtter også multiidentitetsdetektorens funktioner og er derfor en nødvendig komponent for at nå det dobbelte mål om at lette identitetskontrollen af rejsende i god tro og bekæmpe identitetssvig. Adgangen til det fælles identitetsregister til dette formål er begrænset til de brugere, der har brug for oplysningerne til at udføre deres opgaver (hvilket kræver, at disse kontroller bliver et nyt, accessorisk mål for Eurodac, VIS og det fremtidige ind- og udrejsesystem, det foreslåede ETIAS-system og det foreslåede ECRIS-TCN-system). Dataprocessen er strengt begrænset til, hvad der er nødvendigt for at nå dette mål, og der gives tilstrækkelige garantier til at sikre, at adgangsrettighederne respekteres, og de data, der er lagret i det fælles identitetsregister, er det nødvendige minimum. For at sikre dataminimering og undgå uberettiget overlapning af data indeholder det fælles identitetsregister de krævede biografiske oplysninger om hvert af de underliggende systemer – lagret, tilføjet, ændret og slettet i overensstemmelse med deres respektive retsgrundlag – uden

at kopiere dem. Datalagringsvilkårene er i fuld overensstemmelse med bestemmelserne om datalagring i de underliggende informationssystemer, hvor identitetsdataene kommer fra.

Multiidentitetsdetektoren (MID) er nødvendig for at sikre en løsning til påvisning af flere identiteter med det dobbelte formål at lette identitetskontrol for rejsende i god tro og bekæmpe identitetssvig. MID vil indeholde links mellem personer, der findes i mere end ét centralt informationssystem, og være strengt begrænset til de data, der er nødvendige for at verificere, at en person er registreret lovligt eller ulovligt under forskellige personlige identiteter i forskellige systemer, men også for at præcisere, at to personer med samme biografiske data måske ikke er den samme person. Databehandling gennem MID og det fælles BMS med henblik på at sammenkæde individuelle filer på tværs af individuelle systemer holdes på et absolut minimum. MID vil indeholde garantier mod potentiel forskelsbehandling af eller ugunstige afgørelser vedrørende personer med flere lovlige identiteter.

- **Valg af retsakt**

Der stilles forslag om Europa-Parlamentets og Rådets forordning. Den foreslåede lovgivning indeholder direkte bestemmelser om driften af centrale EU-informationssystemer for grænser og sikkerhed, som alle er blevet eller foreslås oprettet i henhold til forordninger. På samme måde er eu-LISA, som skal være ansvarlig for udformningen og udviklingen og med tiden den tekniske forvaltning af komponenterne, også oprettet i henhold til en forordning. En forordning er derfor det korrekte instrument.

3. RESULTATER AF HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

- **Offentlig høring**

Ved udarbejdelsen af dette forslag indledte Kommissionen i juli 2017 en offentlig høring for at indhente synspunkter fra interesserede parter vedrørende interoperabilitet. Under høringen blev der modtaget 18 svar fra en række interessenter, herunder medlemsstaternes regeringer, organisationer i den private sektor, andre organisationer såsom ngo'er og tænketanke såvel som private borgere[33]. Samlet set var svarene stort set positive over for de underliggende principper i dette interoperabilitetsforslag. Langt størstedelen af respondenterne var enige i, at det var de rette spørgsmål, der blev indkredset under høringen, og at det er de rette mål, der søges nået ved hjælp af interoperabilitetspakken. Især fandt respondenterne, at de beskrevne muligheder i høringsdokumentet vil:

- hjælpe medarbejderne på stedet til at få adgang til de oplysninger, de har brug for
- undgå, at de samme oplysninger vises flere gange, reducere overlapninger og fremhæve uoverensstemmelser i data
- identificere personer mere pålideligt – herunder personer med flere identiteter – og reducere identitetssvig.

Et klart flertal af respondenterne gik ind for hver af de foreslåede muligheder og anså dem for at være nødvendige for at nå målene for dette initiativ, idet de i deres svar understregede behovet for stærke og klare bestemmelser om databeskyttelse, navnlig hvad angår adgang til de lagrede oplysninger i systemerne og lagring af data samt behovet for ajourførte data af høj kvalitet i systemerne og foranstaltninger for at sikre dette.

[33] Yderligere oplysninger findes i den sammenfattende rapport, der er vedlagt som bilag til konsekvensanalysen.

Der er ved udarbejdelsen af dette forslag taget hensyn til alle de spørgsmål, der blev rejst.

- **Eurobarometer-undersøgelse**

I juni 2017 blev der gennemført en særlig Eurobarometerundersøgelse[34], der viser, at EU's strategi til udveksling af oplysninger på EU-plan med henblik på at bekæmpe kriminalitet og terrorisme har bred støtte i offentligheden: næsten alle respondenter (92 %) er enige i, at de nationale myndigheder bør udveksle oplysninger med myndighederne i andre medlemsstater for bedre at kunne bekæmpe kriminalitet og terrorisme.

Et klart flertal (69 %) af de adspurgte mente, at politiet og andre nationale retshåndhævende myndigheder systematisk bør udveksle oplysninger med andre EU-lande. I alle medlemsstater mener størstedelen af de adspurgte, at oplysninger under alle omstændigheder skal deles.

- **Ekspertgruppe på højt niveau om informationssystemer og interoperabilitet**

Som allerede anført i indledningen bygger dette forslag på henstillingerne fra **ekspertgruppen på højt niveau vedrørende informationssystemer og interoperabilitet**[35]. Denne gruppe blev oprettet i juni 2016 med det formål at løfte de juridiske, tekniske og operationelle udfordringer i forbindelse med de til rådighed stående muligheder for at opnå interoperabilitet mellem de centrale EU-systemer for grænser og sikkerhed. Gruppen anskuede dataforvaltningsstrukturen for grænsekontrol og retshåndhævelse ud fra et bredt og omfattende perspektiv, idet den også tog hensyn til toldmyndighedernes relevante roller, ansvar og systemer.

Gruppen bestod af eksperter fra medlemsstaterne og associerede Schengenlande og fra EU-agenturerne eu-LISA, Europol, Det Europæiske Asylstøttekontor, Det Europæiske Agentur for Grænse- og Kystbevogtning og EU's Agentur for Grundlæggende Rettigheder. Også EU's antiterrorkoordinator og Den Europæiske Tilsynsførende for Databeskyttelse deltog som fuldgyldige medlemmer af ekspertgruppen. Repræsentanter fra sekretariatet for Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige og Indre Anliggender og Rådets generalsekretariat deltog desuden som observatører.

Den **endelige rapport fra ekspertgruppen på højt niveau** blev offentliggjort i maj 2017[36]. Den understregede behovet for at træffe foranstaltninger for at tage hånd om de strukturelle mangler, som blev kortlagt i meddelelsen fra april 2016. Den indeholdt en række henstillinger for at styrke og udvikle EU's informationssystemer og interoperabilitet. Den konkluderede, at det er **nødvendigt og teknisk gennemførligt at arbejde hen imod en europæisk søgeportal, en fælles biometrisk matchtjeneste og et fælles identitetsregister som løsninger i forbindelse med interoperabilitet**, og at de i princippet kan både sikre operationelle gevinster og oprettes i overensstemmelse med kravene til databeskyttelse. Gruppen anbefalede også at overveje den yderligere mulighed med en totrinstilgang for de retshåndhævende myndigheders adgang på grundlag af en hit/intet hit-påtegning.

---

[34] I rapporten om europæernes holdninger til sikkerhed (*Report on Europeans' attitudes towards security*) analyseres resultaterne af den særlige Eurobarometerundersøgelse (464b) vedrørende borgernes generelle viden om, erfaringer med og opfattelse af sikkerhed. Denne undersøgelse blev gennemført af TNS Political & Social network i de 28 medlemsstater mellem den 13. og 26. juni 2017. Omkring 28 093 EU-borgere fra forskellige sociale grupper og befolkningsgrupper blev interviewet.

[35] Kommissionens afgørelse af 17. juni 2016 om nedsættelse af en ekspertgruppe på højt niveau vedrørende informationssystemer og interoperabilitet – 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

Dette udkast til forordning er også en reaktion på anbefalingerne fra ekspertgruppen på højt niveauvedrørende datakvalitet, det universelle meddelelsesformat (UMF) og oprettelsen af et datalager (her præsenteret som det centrale register for rapportering og statistik (CRRS)).

Den fjerde interoperabilitetskomponent, som foreslås i dette udkast til forordning (multiidentitetsdetektoren), blev ikke nævnt af ekspertgruppen på højt niveau, men opstod i forbindelse med den yderligere tekniske analyse og proportionalitetsvurdering, som Kommissionen foretog.

- **Tekniske undersøgelser**

Der blev indledt tre undersøgelser til støtte for udarbejdelsen af forslaget. Kommissionen bestilte Unisys til at levere en rapport om en gennemførlighedsundersøgelse vedrørende den europæiske søgeportal, og eu-LISA bestilte en teknisk rapport fra Gartner (med Unisys) til støtte for udviklingen af den fælles biometriske matchtjeneste. PWC leverede en teknisk rapport til Kommissionen om et fælles id-register.

- **Konsekvensanalyse**

Dette forslag støttes af en konsekvensanalyse, som præsenteres i det ledsagende arbejdsdokument fra Kommissionens tjenestegrene SWD(2017) 473.

Udvalget for Forskriftskontrol gennemgik konsekvensanalysen på sit møde den 6. december 2017 og afgav sin udtalelse (positiv med forbehold) den 8. december, hvor det anførte, at konsekvensanalysen skulle justeres for at integrere udvalgets anbefalinger om specifikke aspekter. Disse vedrørte dels yderligere foranstaltninger i henhold til den foretrukne valgmulighed for at effektivisere slutbrugernes eksisterende adgangsrettigheder til data i EU-informationssystemer og for at illustrere de tilknyttede garantier for databeskyttelse og grundlæggende rettigheder. Den anden vigtige overvejelse var at afklare, hvordan Schengeninformationssystemet kunne integreres inden for rammerne af valgmulighed 2, herunder hvad angår effektivitet og omkostninger, for at gøre det lettere at sammenligne med den foretrukne valgmulighed 3. Kommissionen ajourførte sin konsekvensanalyse, så den tog højde for disse vigtige overvejelser og for at tage hånd om række andre bemærkninger fra udvalget.

I konsekvensanalysen blev det vurderet, om og hvordan de enkelte udpegede mål kunne nås ved at anvende en eller flere af de tekniske komponenter, som ekspertgruppen på højt niveau havde indkredset, og gennem efterfølgende analyser. Når det var nødvendigt, så den også på de delmuligheder, der er nødvendige for at nå disse mål, samtidig med at databeskyttelsesrammen overholdes. I konsekvensanalysen blev det konkluderet, at:

- For at opfylde målet om at give autoriserede brugere hurtig, problemfri, systematisk og kontrolleret adgang til relevante informationssystemer bør der oprettes en europæisk søgeportal (ESP), der bygger på en fælles biometrisk matchtjeneste (BMS) for alle databaser.
- For at opfylde målet om at lette bemyndigede medarbejderes identitetskontrol af tredjelandsstatsborgere på en medlemsstats område bør der oprettes et fælles identitetsregister, som indeholder et minimumssæt af identifikationsdata og bygger på samme fælles BMS.
- For at opfylde målet om at påvise, at flere identiteter er knyttet til samme sæt biometriske data for derved dels at lette identitetskontrollen af rejsende i god tro, dels

at bekæmpe identitetssvig bør der oprettes en multiidentitetsdetektor (MID), som indeholder links mellem flere identiteter på tværs af systemerne.

- For at opfylde målet om at fremme og effektivisere de retshåndhævende myndigheders adgang til informationssystemer, der ikke vedrører retshåndhævelse, med henblik på at forebygge, efterforske, opdage eller retsforfølge alvorlige strafbare handlinger og terrorisme bør det fælles identitetsregister indeholde en funktion med "hit/intet hit"-påtegninger.

Da alle målene skal opfyldes, er den **fuldstændige løsning en kombination af ESP, det fælles identitetsregister (med hit/intet hit-påtegning) og MID, som alle benytter den fælles BMS**.

Den største positive effekt vil være en forbedring af grænsekontrollen og øget indre sikkerhed i Den Europæiske Union. De nye komponenter vil effektivisere og fremskynde de nationale myndigheders adgang til de nødvendige oplysninger og lette identifikationen af tredjelandsstatsborgere. De vil gøre det muligt for myndighederne at oprette tværgående links til allerede eksisterende, nødvendige oplysninger om enkeltpersoner i forbindelse med ind- og udrejsekontrol, visum- og asylansøgninger samt politiarbejde. Dette vil give adgang til oplysninger, som gør det lettere at træffe pålidelige afgørelser, hvad enten de vedrører efterforskning af alvorlige strafbare handlinger og terrorisme eller afgørelser vedrørende migration og asyl. Selv om de ikke direkte påvirker EU-borgere (de foreslåede foranstaltninger er primært fokuseret på tredjelandsstatsborgere, hvis oplysninger er registreret i et centraliseret informationssystem), ventes forslagene at skabe øget offentlig tillid ved at sikre, at de udformes og anvendes på en måde, der øger EU-borgernes sikkerhed.

Den umiddelbare finansielle og økonomiske virkning af forslaget vil være begrænset til udformningen, udviklingen og driften af de nye komponenter. Omkostningerne skal dækkes over EU-budgettet og af medlemsstaternes myndigheder, der står for driften af systemerne. Indvirkningen på turisme vil være positiv, idet de foreslåede foranstaltninger både vil forbedre sikkerheden i EU og også forventes at sikre en hurtigere grænsekontrol. Ligeledes forventes virkningen på lufthavne, havne og transportvirksomheder at være positiv, navnlig på grund af hurtigere grænsekontrol.

- **Grundlæggende rettigheder**

I konsekvensanalysen blev der især set nærmere på virkningerne af de foreslåede foranstaltninger for de grundlæggende rettigheder og i særdeleshed for retten til databeskyttelse.

Som fastsat i EU's charter om grundlæggende rettigheder, som EU-institutionerne og medlemsstaterne er bundet af, når de gennemfører EU-retten (chartrets artikel 51, stk. 1), skal de muligheder, som interoperabilitet giver som et middel til at øge sikkerheden og beskyttelsen af de ydre grænser, vejes op mod forpligtelsen til at sikre, at indgreb i de grundlæggende rettigheder, som kan forekomme som følge af det nye interoperabilitetsmiljø, er begrænset til, hvad der er strengt nødvendigt for reelt at nå de mål af almen interesse, som forfølges, med forbehold for proportionalitetsprincippet (chartrets artikel 52, stk. 1).

De foreslåede interoperabilitetsløsninger supplerer de eksisterende systemer. De ændrer som sådan ikke den balance, som allerede er sikret i forhold til hvert af de eksisterende centrale systemer med hensyn til deres positive indvirkning på de grundlæggende rettigheder.

Ikke desto mindre kan interoperabilitet have en ekstra, indirekte indvirkning på en række grundlæggende rettigheder. Korrekt identifikation af en person har faktisk en positiv indvirkning på retten til respekt for privatlivet og navnlig retten til ens identitet (chartrets artikel 7), da det kan bidrage til at undgå identitetsforvirring. På den anden side kan kontroller baseret på biometriske data blive opfattet, som om de griber ind i den pågældende persons ret til værdighed (navnlig når det opfattes som ydmygende) (artikel 1). Men i en undersøgelse[37] foretaget af Den Europæiske Unions Agentur for Grundlæggende Rettigheder blev de adspurgte specifikt spurgt, om de mente, at det kunne være ydmygende at udlevere biometriske oplysninger i forbindelse med grænsekontrol. Flertallet af adspurgte mente ikke, at det ville være tilfældet.

De foreslåede interoperabilitetskomponenter giver mulighed for at vedtage målrettede forebyggende foranstaltninger for at øge sikkerheden. Som sådan kan de bidrage til beskyttelsen af menneskers ret til livet (chartrets artikel 2), hvilket også indebærer en positiv forpligtelse for myndighederne til at træffe forebyggende operationelle foranstaltninger for at beskytte en person, hvis liv er i fare, hvis de ved eller burde have vidst, at der forelå en umiddelbar risiko[38], samt til at opretholde forbuddet mod slaveri og tvangsarbejde (artikel 5). Ved hjælp af pålidelig, lettere tilgængelig og enklere identifikation kan interoperabilitet hjælpe med at finde forsvundne børn eller børn, der er ofre for menneskehandel, og fremme hurtige og målrettede reaktioner.

En pålidelig, lettere tilgængelig og enklere identifikation kan også bidrage til at sikre, at asylretten (chartrets artikel 18) og forbuddet mod kollektiv udvisning (chartrets artikel 19) sikres effektivt. Interoperabilitet kan rent faktisk forhindre situationer, hvor asylansøgere pågribes ulovligt, tilbageholdes og gøres til genstand for unødig udvisning. Desuden vil interoperabilitet gøre det lettere at afdække identitetssvig. Det vil også mindske behovet for at dele data og oplysninger om asylansøgere med tredjelande (især oprindelseslandet) med henblik på at fastslå personens identitet og fremskaffe rejsedokumenter, som potentielt kan være til fare for den pågældende person.

- **Beskyttelse af personoplysninger**

Da der er tale om personoplysninger, vil interoperabilitet især få betydning for retten til beskyttelse af personoplysninger. Denne ret er fastsat i chartrets artikel 8, artikel 16 i traktaten om oprettelse af Det Europæiske Union og den europæiske menneskerettighedskonventions artikel 8. Som det understreges af Domstolen[39] udgør retten til beskyttelse af personoplysninger ikke en absolut rettighed, men skal ses i sammenhæng med sin funktion i samfundet[40]. Databeskyttelse hænger tæt sammen med respekten for privatliv og familieliv, som er omhandlet i chartrets artikel 7.

---

[37] *FRA survey in the framework of the eu-LISA pilot on smart borders — travellers' views on and experiences of smart borders*, rapport fra Den Europæiske Unions Agentur for Grundlæggende Rettigheder: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

[38] Den Europæiske Menneskerettighedsdomstol, Osman mod Det Forenede Kongerige, nr. 87/1997/871/1083 af 28. oktober 1998, præmis 116.

[39] EU-Domstolens dom af 9.11.2010, forenede sager C-92/09 og C-93/09, Volker und Markus Schecke og Eifert, Sml. 2010 I, s. 0000.

[40] I overensstemmelse med chartrets artikel 52, stk. 1, kan der indføres begrænsninger i udøvelsen af retten til databeskyttelse, såfremt disse begrænsninger er fastlagt i lovgivningen og respekterer disse rettigheders og friheders væsentligste indhold, og såfremt de under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

Ifølge den generelle databeskyttelsesforordning[41] er den frie bevægelighed for data inden for EU ikke begrænset af hensyn til databeskyttelse. Dog skal en række principper være opfyldt. For at være lovlig skal enhver begrænsning i udøvelsen af de grundlæggende rettigheder, der er beskyttet af chartret, opfylde følgende kriterier, der er fastsat i chartrets artikel 52, stk. 1:

- den skal være fastlagt i lovgivningen
- den skal respektere rettighedernes væsentligste indhold
- den skal svare til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder
- den skal være nødvendig og
- den skal være proportional.

Det nuværende forslag integrerer alle disse databeskyttelsesregler som omhyggeligt beskrevet i den konsekvensanalyse, der ledsager dette forslag til forordning. Forslaget er baseret på principperne om databeskyttelse gennem design og gennem standardindstillinger. Det omfatter alle relevante bestemmelser, der begrænser databehandling til, hvad der er nødvendigt for det specifikke formål, og giver kun adgang til data for de enheder, der har brug for dem. Opbevaringsperioder for data (hvis det er relevant) er passende og begrænsede. Adgangen til data er udelukkende forbeholdt behørigt bemyndigede medarbejdere hos medlemsstaternes myndigheder eller EU-organer, der er kompetente i forhold til de specifikke formål i de enkelte informationssystemer og begrænset til det omfang, hvor der er behov for dataene til at udføre opgaver i overensstemmelse med disse formål.

4. VIRKNINGER FOR BUDGETTET

Virkningerne for budgettet er indeholdt i vedlagte finansieringsoversigt. Den dækker den resterende del af den nuværende flerårige finansielle ramme (indtil 2020) og de syv år af den efterfølgende periode (2021-2027). Det foreslåede budget for årene 2021 og derefter er medtaget som illustration og foregriber ikke den næste flerårige finansielle ramme.

Gennemførelsen af dette forslag vil kræve budgetbevillinger til:

1) **Udvikling** og integration via eu-LISA af de fire interoperabilitetskomponenter og det centrale register til rapportering og statistik samt efterfølgende **vedligeholdelse og drift** af dem.

2) **Overflytning af data** til den fælles biometriske matchtjeneste (fælles BMS) og det fælles identitetsregister. Med hensyn til den fælles BMS skal de biometriske modeller af de tilsvarende data fra de tre systemer, der i øjeblikket bruger biometri (SIS, VIS og Eurodac), genoprettes på den fælles BMS. Med hensyn til det fælles identitetsregister skal personoplysninger fra VIS overflyttes til det fælles identitetsregister, og de mulige links mellem identiteter i SIS, VIS og Eurodac skal valideres. Denne sidste proces er særlig ressourcekrævende.

3) eu-LISA's opdatering af den **nationale ensartede grænseflade**, der allerede er indeholdt i forordningen om ind- og udrejsesystemet, skal blive til en generisk del,

[41] 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).

som muliggør udveksling af meddelelser mellem medlemsstaterne og de(t) centrale system(er).

4) **Integration af medlemsstaternes nationale systemer** og den nationale ensartede grænseflade, som skal videreformidle de meddelelser, der udveksles med det fælles identitetsregister/multiidentitetsdetektoren gennem den europæiske søgeportal.

5) **Uddannelse** af slutbrugerne i anvendelse af interoperabilitetskomponenter, herunder gennem Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse (Cepol).

Interoperabilitetskomponenterne opbygges og vedligeholdes som et program. Mens den europæiske søgeportal (ESP) og multiidentitetsdetektoren er helt nye komponenter sammen med det centrale register til rapportering og statistik (CRRS), er den fælles BMS og det fælles identitetsregister fælles komponenter, som kombinerer eksisterende data, der opbevares (eller vil blive opbevaret) i eksisterende eller nye systemer, med deres nuværende budgetoverslag.

ESP vil udnytte eksisterende, kendte grænseflader for SIS, VIS og Eurodac og vil med tiden blive udvidet til nye systemer.

ESP vil blive brugt af medlemsstaterne og agenturerne ved hjælp af en grænseflade, der er baseret på det universelle meddelelsesformat (UMF). Denne nye grænseflade vil kræve udvikling, tilpasninger, integration og afprøvning i medlemsstaterne og af eu-LISA, Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning. ESP vil anvende koncepterne for en national ensartete grænseflade, der blev indført for ind- og udrejsesystemet, hvilket vil mindske integrationsarbejdet.

ESP vil medføre ekstra omkostninger for Europol, således at QUEST-grænsefladen kan anvendes med data med et grundlæggende beskyttelsesniveau.

Grundlaget for den **fælles BMS** vil de facto blive lagt med oprettelsen af det nye ind- og udrejsesystem, da dette indeholder langt det største antal nye biometriske data. Det nødvendige budget blev reserveret inden for rammerne af retsakten om ind- og udrejsesystemet. Tilføjelse af supplerende biometriske data fra VIS, SIS og Eurodac til den fælles BMS udgør en yderligere omkostning, som hovedsagelig er knyttet til overflytningen af eksisterende data. Omkostningerne hertil skønnes at beløbe sig til 10 mio. EUR for alle tre systemer. Tilføjelse af nye biometriske data fra det foreslåede ECRIS-TCN-system udgør en begrænset ekstraomkostning, der kan dækkes af midler, der er afsat under den foreslåede ECRIS-TCN-retsakt med henblik på at indføre et elektronisk ECRIS-TCN-fingeraftryksidentifikationssystem.

Det fælles identitetsregister vil blive etableret sammen med oprettelsen af det fremtidige ind- og udrejsesystem og udvidet yderligere, når det det foreslåede ETIAS-system udvikles. Udgifterne til lagring af og søgemaskiner for disse data er medtaget i det budget, der blev fastsat i retsakten vedrørende det fremtidige ind- og udrejsesystem og i forslaget vedrørende ETIAS-systemet. Tilføjelse af nye biografiske data fra både Eurodac og det foreslåede ECRIS-TCN-system udgør en mindre ekstraomkostning, som allerede var blevet afsat inden for rammerne af retsakten vedrørende Eurodac og forslagene om ECRIS-TCN-systemet.

Det samlede nødvendige budget over en periode på ni år (2019-2027) beløber sig til 424,7 mio. EUR, der omfatter følgende:

1) Et budget på 225 mio. EUR til eu-LISA, der dækker de samlede omkostninger til programmet for udvikling af de fem interoperabilitetskomponenter (68,3 mio. EUR), omkostningerne til vedligeholdelse fra det tidspunkt, hvor komponenterne leveres og indtil 2027 (56,1 mio. EUR), et specifikt budget på 25 mio. EUR til overflytning af data fra eksisterende systemer til den fælles BMS og ekstraomkostningerne til opdateringen af den nationale ensartede grænseflade, netværk, uddannelse og møder. Et specifikt budget på 18,7 mio. EUR dækker omkostningerne ved opgradering og drift af ECRIS-TCN ved høj tilgængelighed fra 2022.

2) Et budget på 136,3 mio. EUR til de ændringer, medlemsstaterne skal foretage i deres nationale systemer for at kunne bruge interoperabilitetskomponenterne, den nationale ensartede grænseflade leveret af eu-LISA og et budget til uddannelse af slutbrugere.

3) Et budget på 48,9 mio. EUR til Europol til at dække opgraderingen af Europols IT-systemer til den mængde meddelelser, der skal håndteres, og det højere præstationsniveau[42]. Interoperabilitetskomponenterne vil blive anvendt af ETIAS til at søge i Europols oplysninger.

4) Et budget på 4,8 mio. EUR til Det Europæiske Agentur for Grænse- og Kystbevogtning til et team af specialister, som i løbet af et år vil validere links mellem identiteter på det tidspunkt, hvor multiidentitetsdetektoren sættes i drift.

5) Et budget på 2,0 mio. EUR til Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse (Cepol) til dækning af forberedelse og gennemførelse af uddannelse af driftsmedarbejderne.

6) 7,7 mio. EUR til GD Home til dækning af en begrænset forøgelse af personalet og dermed forbundne omkostninger i udviklingsperioden for de forskellige komponenter, eftersom Kommissionen også vil skulle løse andre opgaver i denne periode og tager ansvaret for udvalgets anvendelse af det universelle meddelelsesformat.

Forordningen om Fonden for Intern Sikkerhed er det finansielle instrument, hvori budgettet for gennemførelsen af interoperabilitetsinitiativet er indarbejdet. Den bestemmer i artikel 5, litra b), at 791 mio. EUR skal anvendes til gennemførelsen af et program til udvikling af IT-systemer baseret på eksisterende og/eller nye IT-systemer til forvaltning af migrationsstrømme over EU's ydre grænser, med forbehold af vedtagelsen af de relevante lovgivningsmæssige EU-retsakter og på de betingelser, der er fastsat i artikel 15, stk. 5. Af disse 791 mio. EUR er 480,2 mio. EUR afsat til udvikling af ind- og udrejsesystemet, 210 mio. EUR til ETIAS og 67,9 mio. EUR til revision af SIS. Den resterende del (32,9 mio. EUR) omfordeles ved hjælp af mekanismer inden for rammerne af Fonden for Intern Sikkerhed - grænser. Det nuværende forslag kræver 32,1 mio. EUR for den nuværende flerårige finansielle rammeperiode (2019/2020), som derfor kan dækkes af det resterende budget.

[42] Europols nuværende kapacitet til håndtering af oplysninger er ikke i overensstemmelse med de store mængder (i gennemsnit 100 000 standardsøgninger pr. dag) og den kortere svartid, der vil blive krævet af ETIAS.

5. YDERLIGERE OPLYSNINGER

- **Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering**

eu-LISA er ansvarlig for den operationelle forvaltning af store it-systemer inden for området med frihed, sikkerhed og retfærdighed. Det har allerede fået overdraget driften og de tekniske og driftsmæssige forbedringer af de eksisterende systemer, og udviklingen af de fremtidige systemer er allerede planlagt. I henhold til dette forslag til forordning vil det definere udformningen af den fysiske struktur af interoperabilitetskomponenterne og udvikle og gennemføre dem og i sidste ende hoste dem. De enkelte komponenter vil gradvist blive taget i brug i forbindelse med udviklingen af de underliggende systemer.

Kommissionen vil sikre, at systemerne til overvågning af udviklingen og driften af de fire komponenter (den europæiske søgeportal, den fælles biometriske matchtjeneste, det fælles identitetsregister og multiidentitetsdetektoren) og det centrale register til rapportering og statistik er indført, og evaluere dem i forhold til de vigtigste politiske målsætninger. Fire år efter at funktionerne er indført og sat i drift og derefter hvert fjerde år, forelægger eu-LISA Europa-Parlamentet, Rådet og Kommissionen en rapport om interoperabilitetskomponenternes tekniske funktion. Endvidere skal Kommissionen fem år efter, at funktionerne er indført og fungerer og derefter hvert fjerde år, udarbejde en samlet evaluering af komponenterne, herunder om deres direkte eller indirekte virkninger og deres praktiske konsekvenser for de grundlæggende rettigheder. Den skal gennemgå de opnåede resultater set i forhold til målene og vurdere de grundlæggende princippers fortsatte gyldighed og eventuelle konsekvenser for fremtidige muligheder. Kommissionen bør forelægge evalueringsrapporterne for Europa-Parlamentet og Rådet.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

Kapitel I opstiller de generelle bestemmelser i denne forordning. Det forklarer: de principper, som ligger til grund for forordningen, de komponenter, der er fastsat deri, de mål, der vedrører interoperabilitet, denne forordnings anvendelsesområde, definitioner af de udtryk, der anvendes i denne forordning, og princippet om ikkeforskelsbehandling, for så vidt angår behandling af data i henhold til denne forordning.

Kapitel II indeholder bestemmelser om den europæiske søgeportal (ESP). Dette kapitel indeholder bestemmelser om oprettelse af ESP og dets tekniske struktur, som skal udvikles af eu-LISA. Det præciserer formålet med ESP og fastsætter, hvem der kan anvende ESP, og hvordan de skal anvende den i overensstemmelse med de eksisterende adgangsrettigheder for de enkelte centrale systemer. Der er en bestemmelse om, at eu-LISA skal oprette brugerprofiler for hver kategori af brugere. Dette kapitel beskriver, hvordan der kan søges i centrale systemer via ESP, og foreskriver indholdet og formatet af svar til brugerne. Kapitel II bestemmer ligeledes, at eu-LISA skal føre logfiler over alle databehandlinger, og beskriver en alternativ procedure i tilfælde, hvor ESP ikke kan få adgang til én eller flere af de centrale systemer.

Kapitel III fastsætter bestemmelser for den fælles biometriske matchtjeneste (fælles BMS). Dette kapitel indeholder bestemmelser om oprettelsen af den fælles BMS og dens tekniske struktur, som skal udvikles af eu-LISA. Det angiver formålet med den fælles BMS og beskriver, hvilke data den lagrer. Det forklarer forholdet mellem den fælles BMS og de øvrige komponenter. Kapitel III fastlægger også, at den fælles BMS ikke vil fortsætte med at gemme data, når disse ikke længere findes i de respektive centrale systemer, samt at eu-LISA skal føre logfiler over samtlige behandlinger.

Kapitel IV indeholder bestemmelser om et fælles identitetsregister. Dette kapitel indeholder bestemmelser om oprettelse af det fælles identitetsregister og dets tekniske struktur, som skal udvikles af eu-LISA. Det beskriver målet med det fælles identitetsregister og præciserer, hvilke data der lagres, og hvordan, herunder bestemmelser der skal sikre kvaliteten af de lagrede data. I dette kapitel fastsættes det, at der i det fælles identitetsregister vil blive oprettet individuelle filer baseret på dataene i de centrale systemer, og at de individuelle filer opdateres i overensstemmelse med ændringer i de enkelte centrale systemer. Kapitel IV beskriver også, hvordan det fælles identitetsregister fungerer i forbindelse med multiidentitetsdetektoren. I dette kapitel angives, hvem der kan få adgang til det fælles identitetsregister, og hvordan de kan få adgang til data i overensstemmelse med adgangsrettighederne. Derudover indeholder kapitlet mere specifikke bestemmelser, alt efter om adgangen gives med henblik på identifikation eller, som et første skridt i den todelte strategi, for at få adgang til ind- og udrejsesystemet, VIS, ETIAS og Eurodac via det fælles identitetsregister til retshåndhævelsesformål. I kapitel IV fastsættes det også, at eu-LISA fører logfiler over alle operationer vedrørende det fælles identitetsregister.

Kapitel V indeholder bestemmelser om multiidentitetsdetektoren (MID). Dette kapitel indeholder bestemmelser om oprettelse af MID og dets tekniske struktur, som skal udvikles af eu-LISA. Det forklarer formålet med MID og regulerer anvendelsen af MID i overensstemmelse med adgangsrettighederne til de enkelte centrale systemer. I kapitel V fastsættes det, hvornår og hvordan MID foretager søgninger for at påvise flere identiteter, og hvordan resultaterne leveres, og der skal følges op på dem, herunder om nødvendigt gennem manuel verifikation. Kapitel V indeholder en klassifikation af de typer af links, der kan følge af en søgning, alt efter om resultatet viser en enkelt identitet eller flere identiteter eller fælles identitetsoplysninger. I dette kapitel fastsættes det, at MID vil gemme sammenkædede data lagret i de centrale systemer, mens dataene forbliver i to eller flere individuelle centrale systemer. I kapitel V bestemmes det ligeledes, at eu-LISA skal føre logfiler over alle operationer vedrørende MID.

Kapitel VI indeholder bestemmelser om foranstaltninger til støtte for interoperabilitet. Det indeholder bestemmelser om forbedring af datakvaliteten, indførelsen af det universelle meddelelsesformat som den fælles standard for udveksling af oplysninger, der fremmer interoperabiliteten, og oprettelse af et centralt register til rapportering og statistik.

Kapitel VII vedrører databeskyttelse. Dette kapitel indeholder bestemmelser, som sikrer, at data, der behandles i henhold til denne forordning, behandles lovligt og behørigt, jf. bestemmelserne i forordning (EF) nr. 45/2001. Der redegøres for, hvem der er registerfører for hver af de interoperabilitetsforanstaltninger, der foreslås i denne forordning, og de foranstaltninger, der kræves af eu-LISA og medlemsstaternes myndigheder for at sikre en sikker behandling af data, dataenes fortrolighed, den korrekte håndtering af sikkerhedshændelser og en passende overvågning af overholdelsen af foranstaltningerne i denne forordning skitseres. Kapitlet indeholder også bestemmelser om de registreredes rettigheder, herunder retten til at blive informeret om, at data om dem er blevet lagret og behandlet i henhold til denne forordning, og om retten til at få adgang til, korrigere og slette personoplysninger, der er lagret og behandlet i henhold til denne forordning. Dette kapitel beskriver endvidere princippet om, at data, der behandles i henhold til denne forordning, ikke må overføres til eller stilles til rådighed for et tredjeland, en international organisation eller en privat part med undtagelse af Interpol til visse konkrete formål, og data, der er modtaget fra Europol gennem den europæiske søgeportal, hvor reglerne i forordning (EU) 2016/794 om efterfølgende databehandling finder anvendelse. Endelig indeholder dette kapitel bestemmelser om tilsyn og revision i forbindelse med databeskyttelse.

Kapitel VIII fastsætter ansvarsfordelingen for eu-LISA før og efter idriftsættelsen af foranstaltningerne i dette forslag og for medlemsstaterne, Europol og ETIAS' centrale enhed.

Kapitel IX vedrører ændringer af andre EU-retsakter. Dette kapitel introducerer de ændringer af andre retsforskrifter, der er nødvendige for at sikre en fuldstændig gennemførelse af dette forslag om interoperabilitet. Forslaget indeholder detaljerede bestemmelser om de nødvendige ændringer af de retlige instrumenter, der for øjeblikket er stabile tekster vedtaget af Europa-Parlamentet og Rådet: Schengengrænsekodeksen, forordningen om ind- og udrejsesystemet, VIS-forordningen (EF), Rådets afgørelse 2004/512/EF (VIS-afgørelsen) og Rådets afgørelse 2008/633/RIA (afgørelsen om VIS/adgang for retshåndhævende myndigheder).

Kapitel X indeholder nærmere bestemmelser vedrørende: statistik- og rapporteringskrav vedrørende data, der behandles i henhold til denne forordning, overgangsforanstaltninger, der vil være påkrævet, ordninger vedrørende omkostninger, der følger af denne forordning, krav vedrørende meddelelser, processen for påbegyndelse af foranstaltningerne i denne forordning, styringsordninger, herunder nedsættelse af et udvalg og en rådgivende gruppe, eu-LISA's ansvar i forhold til uddannelse og en praktisk håndbog til støtte for gennemførelsen og forvaltningen af interoperabilitetskomponenterne, procedurerne for overvågning og evaluering af de foranstaltninger, der er foreslået i denne forordning, og bestemmelser om denne forordnings ikrafttræden.

2017/0351 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om fastsættelse af en ramme for interoperabiliteten mellem EU-informationssystemer (grænser og visum) og om ændring af Rådets afgørelse 2004/512/EF, forordning (EF) nr. 767/2008, Rådets afgørelse 2008/633/RIA, forordning (EU) 2016/399 og forordning (EU) 2017/2226

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 77, stk. 2, litra a), b), d) og e),

under henvisning til forslag fra Europa-Kommissionen,

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

efter høring af Den Europæiske Tilsynsførende for Databeskyttelse, og

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[43],

under henvisning til udtalelse fra Regionsudvalget[44],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) I sin meddelelse af 6. april 2016 om stærkere og mere intelligente informationssystemer for grænser og sikkerhed[45] understregede Kommissionen nødvendigheden af at forbedre EU's dataforvaltningsstruktur for grænsekontrol og sikkerhed. Meddelelsen indledte en proces med henblik på at opnå interoperabilitet mellem EU's 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[46] kortlagde Rådet forskellige juridiske, tekniske og driftsmæssige udfordringer i forbindelse med EU-informationssystemernes interoperabilitet og opfordrede til at finde løsninger.

(3) I sin beslutning af 6. juli 2016 om de strategiske prioriteringer for Kommissionens arbejdsprogram for 2017[47] opfordrede Europa-Parlamentet Kommissionen til at

[43] EUT C , , s. .

[44]

[45] COM(2016) 205 af 6.4.2016.

[46] Køreplan af 6. juni 2016 til styrkelse af informationsudveksling og informationsstyring, herunder interoperabilitetsløsninger på området for retlige og indre anliggender – 9368/1/16 REV 1.

[47] Europa-Parlamentets beslutning af 6. juli 2016 om de strategiske prioriteringer for Kommissionens arbejdsprogram for 2017 (2016/2773 (RSP)).

fremsætte forslag til at forbedre og udvikle eksisterende 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) Det Europæiske Råd af 15. december 2016[48] opfordrede til fortsat at levere resultater med hensyn til EU-informationssystemers og -databasers interoperabilitet.

(5) Ekspertgruppen på højt niveau konkluderede i sin endelige rapport af 11. maj 2017[49], at det er nødvendigt og teknisk gennemførligt at arbejde hen imod praktiske interoperabilitetsløsninger, og at de 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"[50] 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 data for grænser, sikkerhed og migration, hvor alle EU-informationssystemer for sikkerhed, grænse- og migrationsforvaltning er interoperable med fuld respekt for de grundlæggende rettigheder.

(7) I sine konklusioner af 9. juni 2017[51] om forbedring af udvekslingen af oplysninger og sikring af EU-informationssystemernes interoperabilitet opfordrede Rådet Kommissionen til at forfølge de interoperabilitetsløsninger, som ekspertgruppen på højt niveau havde foreslået.

(8) Det Europæiske Råd af 23. juni 2017[52] understregede behovet for at forbedre interoperabiliteten mellem databaser og opfordrede Kommissionen til snarest muligt at udarbejde udkast til lovgivning til vedtagelse af de forslag, som er fremsat af ekspertgruppen på højt niveau vedrørende informationssystemer og interoperabilitet.

(9) Med henblik på at forbedre forvaltningen af de ydre grænser, bidrage til at forebygge og bekæmpe ulovlig migration og bidrage til et højt sikkerhedsniveau inden for området med frihed, sikkerhed og retfærdighed i Unionen, herunder opretholdelse af den offentlige sikkerhed og den offentlige orden og beskyttelse af sikkerhed i medlemsstaterne, 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 data supplerer hinanden. For at opnå dette bør der oprettes en europæisk søgeportal (ESP), en fælles biometrisk matchtjeneste (fælles BMS), et fælles identitetsregister og en multiidentitetsdetektor (MID) som interoperabilitetskomponenter.

(10) Interoperabiliteten mellem EU-informationssystemerne bør gøre det muligt for disse systemer at supplere hinanden for at lette en korrekt identifikation af personer, bidrage til at bekæmpe identitetssvig, forbedre og harmonisere datakvalitetskravene i de enkelte EU-informationssystemer, lette den tekniske og praktiske gennemførelse i

---

48 http://www.consilium.europa.eu/da/press/press-releases/2016/12/15/euco-conclusions-final/.
49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
50 COM(2017) 261 final af 16.5.2017.
51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.
52 Det Europæiske Råds konklusioner, 22.-23.6.2017.

medlemsstaterne af EU's nuværende og fremtidige informationssystemer, styrke og forenkle datasikkerheden og de databeskyttelsesregler, der gælder for de respektive EU-informationssystemer, effektivisere de retshåndhævende myndigheders adgang til ind- og udrejsesystemet, VIS, [ETIAS] og Eurodac samt støtte formålene med ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS og [ECRIS-TCN-systemet].

(11) Interoperabilitetskomponenterne bør omfatte ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS og [ECRIS-TCN-systemet]. De bør også omfatte Europol-dataene, i det omfang det giver mulighed for at søge i disse samtidig med EU-informationssystemerne.

(12) Interoperabilitetskomponenterne bør vedrøre personer, om hvem der kan være behandlet personoplysninger i EU-informationssystemerne og af Europol, nemlig tredjelandsstatsborgere, hvis personoplysninger behandles i EU's informationssystemer og af Europol, og EU-borgere, hvis personoplysninger behandles i SIS og af Europol.

(13) Den europæiske søgeportal (ESP) bør oprettes således, at den giver medlemsstaternes myndigheder og EU-organerne bedre mulighed for at opnå hurtig, problemfri, effektiv, systematisk og kontrolleret adgang til de EU-informationssystemer, Europol-data og Interpol-databaser, som de skal bruge for at udføre deres opgaver i overensstemmelse med deres adgangsrettigheder, og støtter formålene med ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN-systemet] og Europol-dataene. Ved at gøre det muligt at søge samtidig i alle relevante EU-informationssystemer parallelt samt i Europol-dataene og Interpol-databaserne skal ESP fungere som en enkelt grænseflade eller "meddelelsesformidler" med hensyn til at søge i forskellige centrale systemer og udtrække de nødvendige oplysninger problemfrit og under fuld overholdelse af de underliggende systemers krav til adgangskontrol og databeskyttelse.

(14) Den Internationale Kriminalpolitiorganisations (Interpols) database over stjålne og bortkomne rejsedokumenter gør det muligt for godkendte retshåndhævelsesenheder i medlemsstaterne, herunder migrations- og grænsekontrolmedarbejdere, at fastslå gyldigheden af et rejsedokument. Via [ETIAS] søges der i databasen over stjålne og bortkomne rejsedokumenter og Interpols database over rejsedokumenter med tilknyttede notifikationer (TDAWN) for at vurdere, om det er sandsynligt, at en person, der ansøger om rejsetilladelse, er en irregulær migrant eller kan udgøre en trussel mod sikkerheden. Den centrale europæiske søgeportal (ESP) bør gøre det muligt at søge i databasen over stjålne og bortkomne rejsedokumenter og TDAWN ved hjælp af en persons identitetsdata. Hvis personoplysninger overføres fra Unionen til Interpol gennem ESP, bør bestemmelserne om internationale overførsler i kapitel V i Europa-Parlamentets og Rådets forordning (EU) 2016/679[53] eller de nationale bestemmelser, der gennemfører kapitel V i Europa-Parlamentets og Rådets direktiv

[53] 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).

(EU) 2016/680[54], finde anvendelse. Dette bør ikke berøre de specifikke regler, der er fastsat i Rådets fælles holdning 2005/69/RIA[55] og Rådets afgørelse 2007/533/RIA[56].

(15) Den europæiske søgeportal (ESP) bør udvikles og konfigureres på en sådan måde, at det ikke er muligt at anvende datafelter til søgninger, som ikke vedrører personer eller rejsedokumenter, eller som ikke findes i et EU-informationssystem, i Europol-dataene eller Interpol-databasen.

(16) For at sikre hurtig og systematisk brug af alle EU-informationssystemer bør den europæiske søgeportal (ESP) anvendes til søgninger i det fælles identitetsregister, ind- og udrejsesystemet, VIS, [ETIAS], Eurodac og [ECRIS-TCN-systemet]. Den nationale forbindelse til de forskellige EU-informationssystemer bør dog fastholdes som et teknisk sikkerhedsnet. EU-organerne bør ligeledes anvende ESP til at søge i det centrale SIS i overensstemmelse med deres adgangsrettigheder og for at udføre deres opgaver. ESP bør være et supplerende middel til søgninger i det centrale SIS, Europol-dataene og Interpol-systemerne og supplere de eksisterende specifikke grænseflader.

(17) Biometriske data såsom fingeraftryk og ansigtsbilleder er unikke og derfor meget mere pålidelige end alfanumeriske data til at identificere en person. Den fælles biometriske matchtjeneste (fælles BMS) bør være et teknisk redskab, der skal 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 kan være registreret i forskellige databaser, ved at matche dennes biometriske data på tværs af forskellige systemer og ved at anvende en unik teknologisk komponent i stedet for fem forskellige i hvert af de underliggende systemer. Den fælles BMS bør både bidrage til sikkerheden og give finansielle, vedligeholdelsesmæssige og driftsmæssige fordele ved at anvende en unik teknologisk komponent i stedet for forskellige i hvert af de underliggende systemer. Alle elektroniske fingeraftryksidentifikationssystemer, herunder dem, der i øjeblikket anvendes til Eurodac, VIS og SIS, anvender biometriske skabeloner, der består af data, der udledes af faktiske biometriske prøver. Den fælles BMS burde omgruppere og lagre alle disse biometriske skabeloner på ét enkelt sted for at lette sammenligninger på tværs af systemer ved hjælp af biometriske data og give stordriftsfordele med hensyn til at udvikle og opretholde EU's centrale systemer.

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

(19) De systemer, der oprettes ved Europa-Parlamentets og Rådets forordning (EU) 2017/2226[57], Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008[58], [ETIAS-

---

[54] 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).

[55] Rådets fælles holdning 2005/69/RIA af 24. januar 2005 om udveksling af bestemte oplysninger med Interpol (EUT L 27 af 29.1.2005, s. 61).

[56] Rådets afgørelse 2007/533/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 205 af 7.8.2007, s. 63).

[57] 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

forordningen] om forvaltning af Unionens grænser, det system, der er indført ved [Eurodac-forordningen] for at identificere ansøgere om international beskyttelse og bekæmpe irregulær migration, og det system, der er indført ved [forordningen om ECRIS-TCN-systemet], kræver for at være effektive, at der sker en præcis identifikation af de tredjelandsstatsborgere, hvis personoplysninger er lagret heri.

(20) Det fælles identitetsregister bør derfor lette og understøtte en korrekt identifikation af personer, der er registreret i ind- og udrejsesystemet, VIS, [ETIAS], Eurodac og [ECRIS-TCN-systemet].

(21) 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 i deres område, men det samme er ikke tilfældet for tredjelandsstatsborgere. Interoperabiliteten mellem EU-informationssystemerne bør bidrage til en korrekt identifikation af tredjelandsstatsborgere. Det fælles identitetsregister bør lagre de personoplysninger om tredjelandsstatsborgere i disse systemer, der er nødvendige for at foretage en mere præcis identifikation af disse personer, nemlig bl.a. deres identitet, rejsedokumenter og biometriske data, uanset i hvilket system dataene oprindeligt blev indsamlet. Kun de personoplysninger, der er strengt nødvendige for at foretage en nøjagtig identitetskontrol, bør opbevares i det fælles identitetsregister. De personoplysninger, der er registreret i det fælles identitetsregister, bør kun opbevares så længe, det er strengt nødvendigt med henblik på de underliggende systemer, og bør slettes automatisk, når dataene slettes i de underliggende systemer i overensstemmelse med deres logiske adskillelse.

(22) Den nye behandling, der består i at lagre disse data i det fælles identitetsregister i stedet for at lagre dem i hvert af de særskilte systemer, er nødvendig for at øge nøjagtigheden af den identifikation, der muliggøres med den elektroniske sammenligning og matchning af sådanne data. At identiteten på og de biometriske data for tredjelandsstatsborgere lagres i det fælles identitetsregister bør ikke på nogen måde være til hinder for behandlingen af data med henblik på forordningerne om ind- og udrejsesystemet, VIS, ETIAS, Eurodac eller ECRIS-TCN-systemet, eftersom det fælles identitetsregister vil være en ny fælles komponent for disse underliggende systemer.

(23) I denne forbindelse er det nødvendigt at oprette en enkelt fil i det fælles identitetsregister for hver person, der registreres i ind- og udrejsesystemet, VIS, ETIAS, Eurodac eller ECRIS-TCN-systemet, for at opfylde formålet med korrekt identifikation af tredjelandsstatsborgere inden for Schengenområdet og for at støtte multiidentitetsdetektorens dobbelte formål, nemlig at lette identitetskontrol for rejsende i god tro og bekæmpe identitetssvig. Den enkelte fil bør lagres et enkelt sted og give alle behørigt autoriserede slutbrugere adgang til alle de mulige identiteter, der er knyttet til en person.

(24) Det fælles identitetsregister bør derfor understøtte multiidentitetsdetektorens funktionsmåde og lette og effektivisere de retshåndhævende myndigheders adgang til

---

konventionen om gennemførelse af Schengenaftalen og forordning (EF) nr. 767/2008 og (EU) nr. 1077/2011 (forordningen om ind- og udrejsesystemet) (EUT L 327 af 9.12.2017, s. 20-82).

[58] 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).

de EU-informationssystemer, der ikke er oprettet udelukkende med henblik på forebyggelse, efterforskning, opdagelse eller retsforfølgning af grov kriminalitet.

(25) Det fælles identitetsregister bør være et fælles register over identitetsdata og biometriske data for tredjelandsstatsborgere, der er registreret i ind- og udrejsesystemet, VIS, [ETIAS], Eurodac og [ECRIS-TCN-systemet], og fungere som den fælles komponent mellem disse systemer til lagring af disse data og muliggøre søgninger deri.

(26) Alle registreringer i det fælles identitetsregister bør adskilles logisk ved automatisk at markere de enkelte registreringer med det underliggende system, der ejer registreringen. Adgangskontrollen til det fælles identitetsregister bør anvende disse markeringer til at markere, om registreringen er tilgængelig eller ej.

(27) For at sikre en korrekt identifikation af en person skal medlemsstaternes kompetente myndigheder med ansvar for forebyggelse og bekæmpelse af irregulær migration og de kompetente myndigheder i henhold til artikel 3, stk. 7, i direktiv 2016/680 have mulighed for at foretage søgninger i det fælles identitetsregister med den pågældende persons biometriske data, som blev indsamlet under en identitetskontrol.

(28) Hvis en persons biometriske data ikke kan bruges, eller hvis søgningen med disse data ikke lykkes, bør søgningen foretages med identitetsdata for den pågældende person i kombination med rejsedokumentdata. Hvis søgningen viser, at data om denne person er lagret i det fælles identitetsregister, bør medlemsstaternes myndigheder have adgang til denne persons identitetsdata, som er lagret i det fælles identitetsregister, uden at skulle angive, hvilket EU-informationssystem dataene findes i.

(29) Medlemsstaterne bør vedtage nationale lovgivningsmæssige foranstaltninger for at udpege de kompetente myndigheder, der skal foretage identitetskontrol ved hjælp af det fælles identitetsregister, og fastsætte procedurer, betingelser og kriterier for kontrollen i overensstemmelse med proportionalitetsprincippet. Især bør beføjelserne for en ansat hos disse myndigheder til at indsamle biometriske data under en identitetskontrol af en person fastsættes i national lovgivning.

(30) Med denne forordning bør også indføres en ny mulighed for mere effektiv adgang til data ud over de identitetsdata, der findes i ind- og udrejsesystemet, VIS, [ETIAS] eller Eurodac, for de retshåndhævende myndigheder, der er udpeget af medlemsstaterne, og Europol. Data, herunder andre data end identitetsdata i disse systemer, kan være nødvendige for at forebygge, opdage, efterforske og retsforfølge terrorhandlinger eller alvorlige strafbare handlinger i en konkret sag.

(31) Fuld adgang til andre nødvendige data, der er indeholdt i EU-informationssystemerne, som er nødvendige med henblik på at forebygge, opdage og efterforske terrorhandlinger eller andre alvorlige strafbare handlinger end de relevante identitetsdata, der er omfattet af det fælles identitetsregister, og som er indsamlet ved hjælp af biometriske data for denne person under en identitetskontrol, bør fortsat være omfattet af bestemmelserne i de respektive retsakter. De udpegede retshåndhævende myndigheder og Europol ved ikke på forhånd, hvilke af EU-informationssystemerne der indeholder data om de personer, de har brug for at forespørge om. Dette resulterer i forsinkelser og ineffektivitet, når de skal udføre deres opgaver. En slutbruger, som er godkendt af den udpegede myndighed, bør derfor have lov til at se, i hvilke af EU-informationssystemerne dataene, der svarer til forespørgslen, er registreret. Det pågældende system vil dermed blive markeret efter den automatiske verifikation af, om der er et hit i systemet (en såkaldt hit/intet hit-påtegning).

(32) Logfilerne over forespørgsler i det fælles identitetsregister bør vise formålet med forespørgslen. Hvis en sådan forespørgsel blev udført ved hjælp af totrinstilgangen, bør logfilerne indeholde en henvisning til den nationale fil for undersøgelsen eller sagen og derfor angive, at forespørgslen blev foretaget med henblik på at forebygge, opdage og efterforske terrorhandlinger og andre alvorlige strafbare handlinger.

(33) Forespørgsler i det fælles identitetsregister fra medlemsstaternes udpegede myndigheder og Europol med henblik på at opnå et svar med hit-påtegning, der angiver, at dataene er registreret i ind- og udrejsesystemet, VIS, [ETIAS] eller Eurodac, kræver elektronisk behandling af personoplysninger. En hit-påtegning vil ikke vise personoplysninger om den pågældende person, men blot angive, at nogle af dennes data er lagret i et af systemerne. Den autoriserede slutbruger bør ikke træffe nogen negativ afgørelse vedrørende den pågældende person alene på grundlag af den simple forekomst af en hit-påtegning. Slutbrugerens adgang til en hit-påtegning vil derfor være et meget begrænset indgreb i retten til beskyttelse af personoplysninger om den pågældende person, men det vil være nødvendigt at give den udpegede myndighed og Europol lov til at håndtere anmodningen om adgang til personoplysninger mere effektivt direkte i det system, som ifølge påtegningen indeholder dem.

(34) Totrinstilgangen er navnlig værdifuld i de tilfælde, hvor en mistænkt, en gerningsmand eller et formodet offer for en terrorhandling eller en anden alvorlig strafbar handling er ukendt. I disse tilfælde bør det fælles identitetsregister gøre det muligt at finde det informationssystem, som indeholder oplysninger om den pågældende person, i en enkelt søgning. Ved at gøre det obligatorisk for de retshåndhævende myndigheder at bruge denne nye tilgang i sådanne tilfælde bør adgangen til de personoplysninger, der er lagret i ind- og udrejsesystemet, VIS, [ETIAS] og Eurodac, ske uden krav om en forudgående søgning i de nationale databaser og indledning af en forudgående søgning i andre medlemsstaters elektroniske fingeraftryksidentifikationssystem i henhold til afgørelse 2008/615/RIA. Princippet om forudgående søgning begrænser effektivt muligheden for, at medlemsstaternes myndigheder kan benytte systemer i forbindelse med begrundede retshåndhævelsesformål, og kan dermed resultere i, at de mister muligheden for at finde frem til de nødvendige oplysninger. Kravene om en forudgående søgning i de nationale databaser og indledningen af en forudgående søgning i andre medlemsstaters elektroniske fingeraftryksidentifikationssystemer i henhold til afgørelse 2008/615/RIA bør kun ophøre med at gælde, når den alternative sikkerhedsforanstaltning i form af totrinstilgangen til de retshåndhævende myndigheders adgang gennem det fælles identitetsregister er taget i brug.

(35) Multiidentitetsdetektoren (MID) bør oprettes for at støtte det fælles identitetsregisters funktion og målene for ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS og [ECRIS-TCN-systemet]. For at alle disse EU-informationssystemer effektivt kan opfylde deres formål, kræves der en præcis identifikation af de personer, hvis personoplysninger er lagret deri.

(36) Muligheden for at nå målene for EU-informationssystemerne bringes i fare, fordi myndighederne på nuværende tidspunkt ikke kan anvende disse systemer til at foretage en tilstrækkeligt pålidelig verifikation af identiteten på de tredjelandsstatsborgere, hvis data er lagret i de forskellige systemer. Dette skyldes, at de identitetsdata, som er lagret i et givet individuelt system, kan være svigagtige, ukorrekte eller ufuldstændige, og at der i øjeblikket ingen mulighed er for at opdage sådanne svigagtige, ukorrekte eller ufuldstændige identitetsdata ved at sammenligne

med data, 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 præcist at identificere tredjelandsstatsborgere til disse formål.

(37) Multiidentitetsdetektoren (MID) bør oprette og lagre links mellem data i de forskellige EU-informationssystemer med henblik på at påvise flere identiteter, både for at lette identitetskontrollen af rejsende i god tro og bekæmpe identitetssvig. MID bør kun indeholde links mellem personer, der optræder i mere end ét EU-informationssystem, og være strengt begrænset til de data, som er nødvendige for at verificere, at en person er registreret lovligt eller ulovligt under forskellige biografiske identiteter i forskellige systemer, eller for at præcisere, at to personer med lignende biografiske data måske ikke er den samme person. Databehandling gennem den europæiske søgeportal (ESP) og den fælles biometriske matchtjeneste (fælles BMS) for at forbinde de enkelte filer på tværs af de individuelle systemer bør holdes på et absolut minimum og er derfor begrænset til påvisning af flere identiteter på det tidspunkt, hvor nye data føjes til et af de informationssystemer, der indgår i det fælles identitetsregister og i SIS. MID bør omfatte sikkerhedsforanstaltninger mod potentiel forskelsbehandling eller ugunstige afgørelser vedrørende personer med flere lovlige identiteter.

(38) Denne forordning indeholder bestemmelser om nye databehandlinger til korrekt identifikation af de pågældende personer. Dette udgør et indgreb i deres grundlæggende rettigheder, som er beskyttet af artikel 7 og 8 i chartret om grundlæggende rettigheder. Eftersom en effektiv gennemførelse af EU-informationssystemerne afhænger af, at der foretages en korrekt identifikation af de pågældende personer, er et sådant indgreb begrundet i de samme mål, som hvert af disse systemer er blevet oprettet for, nemlig effektiv forvaltning af Unionens grænser, den interne sikkerhed i Unionen, effektiv gennemførelse af Unionens asyl- og visumpolitik og bekæmpelse af irregulær migration.

(39) Den europæiske søgeportal (ESP) og den fælles biometriske matchtjeneste (fælles BMS) bør sammenligne data i det fælles identitetsregister og SIS om personer, når en national myndighed eller et EU-organ foretager nye registreringer. Denne sammenligning bør automatiseres. Det fælles identitetsregister og SIS bør bruge den fælles BMS til at opdage mulige links på grundlag af biometriske data. Det fælles identitetsregister og SIS bør bruge ESP til at opdage mulige links på grundlag af alfanumeriske data. Det fælles identitetsregister og SIS bør være i stand til at identificere identiske eller lignende data om tredjelandsstatsborgere, der er lagret i flere forskellige systemer. Når det er tilfældet, bør der oprettes et link, der angiver, at det er den samme person. Det fælles identitetsregister 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 tredjelandsstatsborger.

(40) Den nationale myndighed eller det EU-organ, der registrerede dataene i det respektive EU-informationssystem, bør bekræfte eller ændre disse links. Denne myndighed bør have adgang til de data, der er lagret i det fælles identitetsregister eller SIS og i multiidentitetsdetektoren (MID) med henblik på manuel identitetsverifikation.

(41) Adgangen til multiidentitetsdetektoren (MID) for medlemsstaternes myndigheder og de EU-organer, der har adgang til mindst ét EU-informationssystem i det fælles identitetsregister eller til SIS, bør begrænses til såkaldt røde links, hvor de sammenkædede data har samme biometriske data, men forskellige identitetsdata, og den myndighed, der er ansvarlig for verifikationen af forskellige identiteter, har konkluderet, at de henviser ulovligt til den samme person, eller hvor de

sammenkædede data har en tilsvarende dataidentitet, og den myndighed, der har ansvaret for verifikationen af forskellige identiteter, har konkluderet, at de henviser ulovligt til den samme person. Såfremt de sammenkædede identitetsdata ikke er ens, bør der oprettes et gult link, og der bør foretages en manuel verifikation for at bekræfte linket eller ændre farven i overensstemmelse hermed.

(42) Den manuelle verifikation af flere identiteter bør sikres af den myndighed, der har indlæst eller ajourført de data, der udløste et hit, der resulterede i et link til data, der allerede er lagret i et andet EU-informationssystem. Den myndighed, der er ansvarlig for verifikationen af flere identiteter, bør vurdere, om der er flere lovlige eller ulovlige identiteter. En sådan vurdering bør så vidt muligt foretages i nærværelse af tredjelandsstatsborgeren og om nødvendigt ved at anmode om yderligere præciseringer eller oplysninger. En sådan vurdering bør udføres straks i overensstemmelse med de retlige krav med hensyn til rigtigheden af oplysninger i henhold til EU-retten og national ret.

(43) Med hensyn til de opnåede links til Schengeninformationssystemet (SIS) vedrørende indberetninger om personer, der er eftersøgte med henblik på anholdelse, overgivelse eller udlevering, indberetninger om forsvundne eller sårbare personer, om personer, der eftersøges med henblik på at yde bistand i forbindelse med en retssag, om personer, der er genstand for diskret kontrol eller målrettet kontrol, eller om ukendte eftersøgte personer, bør den ansvarlige myndighed for verifikationen af flere 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 dataene i et af de andre EU-informationssystemer. Oprettelsen af et link til SIS-data bør ikke berøre de foranstaltninger, der skal træffes i overensstemmelse med [SIS-forordningerne].

(44) 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 gennemførelsen og anvendelsen af EU-informationssystemerne i medlemsstaterne. De fælles kvalitetsindikatorer bør omfatte minimumskvalitetsstandarderne for at lagre data i EU-informationssystemerne eller interoperabilitetskomponenterne. Målet med sådanne datakvalitetsstandarder bør være, at EU-informationssystemerne og interoperabilitetskomponenterne automatisk kan finde tilsyneladende forkerte eller inkonsekvente dataregistreringer, så den medlemsstat, hvorfra dataene kommer, kan verificere dataene og træffe eventuelle nødvendige afhjælpende foranstaltninger.

(45) Kommissionen bør evaluere eu-LISA's kvalitetsrapporter og om nødvendigt 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 deres fremskridt.

(46) Det universelle meddelelsesformat (UMF) bør fastsættes som standard for struktureret, grænseoverskridende informationsudveksling mellem informationssystemer, myndigheder og/eller organisationer på området for retlige og indre anliggender. Via UMF bør der fastsættes et fælles ordforråd og logiske strukturer til almindeligt udvekslede oplysninger med det formål at lette interoperabiliteten, således at indholdet af de udvekslede oplysninger kan fastsættes og læses på en konsekvent og semantisk ækvivalent måde.

(47) Der bør oprettes et centralt register til rapportering og statistik (CRRS), der skal generere statistiske data og analytisk rapportering på tværs af systemerne til politiske, operationelle og datakvalitetsmæssige formål. eu-LISA bør indføre, gennemføre og hoste CRRS på sine tekniske websteder, der indeholder anonyme statistiske oplysninger fra de ovennævnte systemer, det fælles identitetsregister, multiidentitetsdetektoren og den fælles biometriske matchtjeneste. De data, der er indeholdt i CRRS, bør ikke gøre det muligt at identificere enkeltpersoner. eu-LISA bør udlevere dataene anonymt og registrere sådanne anonyme data i CRRS. Processen med at anonymisere data bør automatiseres, og eu-LISA's personale bør ikke gives direkte adgang til personoplysninger, som er lagret i EU-informationssystemerne eller i interoperabilitetskomponenterne.

(48) Forordning (EU) 2016/679 bør finde anvendelse på de nationale myndigheders behandling af personoplysninger i henhold til denne 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, hvor Europa-Parlamentets og Rådets direktiv (EU) 2016/680 bør finde anvendelse.

(49) De særlige bestemmelser om databeskyttelse i [forordningen om ind- og udrejsesystemet], forordning (EF) nr. 767/2008, [ETIAS-forordningen] og [SIS-forordningen inden for grænsekontrol] bør finde anvendelse på behandlingen af personoplysninger i de respektive systemer.

(50) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001[59] bør finde anvendelse på behandlingen af personoplysninger i eu-LISA og andre EU-institutioner og -organer, når de udfører deres opgaver i henhold til denne forordning, uden at det berører forordning (EU) 2016/794, som bør finde anvendelse på behandlingen af personoplysninger i Europol.

(51) De nationale tilsynsmyndigheder, som er oprettet i henhold til [forordning (EU) 2016/679], bør kontrollere, at medlemsstaternes behandling af personoplysninger er lovlig, mens Den Europæiske Tilsynsførende for Databeskyttelse, som er oprettet ved forordning (EF) nr. 45/2001, bør kontrollere 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.

(52) "(...) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt i henhold til artikel 28, stk. 2, i forordning (EF) nr. 45/2001, og afgav udtalelse den [...]."

(53) For så vidt angår fortrolighed bør de relevante bestemmelser i vedtægten for tjenestemænd i Den Europæiske Union og ansættelsesvilkårene for Unionens øvrige ansatte finde anvendelse på de tjenestemænd og øvrige ansatte, hvis arbejde har forbindelse til SIS.

(54) 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 dataintegriteten for så vidt angår udvikling, udformning og styring af interoperabilitetskomponenterne.

[59] 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).

(55) Gennemførelsen af de interoperabilitetskomponenter, der er fastsat bestemmelser om i denne forordning, vil påvirke den måde, hvorpå der foretages kontrol ved grænseovergangene. Det vil være resultatet af en kombineret anvendelse af de eksisterende regler i Europa-Parlamentets og Rådets forordning (EU) 2016/399[60] og reglerne om interoperabilitet i henhold til denne forordning.

(56) Som følge af denne kombinerede anvendelse af reglerne bør den europæiske søgeportal (ESP) udgøre det vigtigste adgangspunkt for obligatorisk systematisk søgning i databaser efter oplysninger om tredjelandsstatsborgere ved grænseovergange i henhold til Schengengrænsekodeksen. Derudover bør de identitetsdata, der førte til klassificeringen af et link i multiidentitetsdetektoren (MID) som et rødt link, tages i betragtning af grænsevagterne for at vurdere, hvorvidt personen opfylder betingelserne for indrejse som fastsat i Schengengrænsekodeksen. Det forhold. at der er et rødt link, udgør dog ikke i sig selv en begrundelse for at nægte indrejse, og de eksisterende grunde til at nægte indrejse i henhold til Schengengrænsekodeksen bør derfor ikke ændres.

(57) Det vil være hensigtsmæssigt at ajourføre den praktiske vejledning for grænsevagter for at præcisere dette.

(58) Dog vil der være behov for en ændring af forordning (EU) 2016/399 for at tilføje forpligtelsen for grænsevagterne til at henvise en tredjelandsstatsborger til kontrol i anden linje, såfremt anvendelsen af multiidentitetsdetektoren (MID) via den europæiske søgeportal (ESP) viser et gult eller rødt link, for ikke at forlænge ventetiden ved kontrollen i første linje.

(59) Hvis forespørgslen i multiidentitetsdetektoren (MID) gennem den europæiske søgeportal (ESP) resulterer i et gult link eller viser et rødt link, bør grænsevagten i anden linje benytte det fælles identitetsregister eller Schengeninformationssystemet eller begge til at vurdere oplysningerne om den person, der kontrolleres, for manuelt at verificere dennes anden identitet og tilpasse farven på linket, hvis det er nødvendigt.

(60) For at understøtte både statistik og rapportering er det nødvendigt at give adgang til bemyndigede medarbejdere i de kompetente myndigheder, institutioner og organer, der er fastsat i denne forordning, så de kan benytte visse data vedrørende visse interoperabilitetskomponenter uden at give mulighed for identifikation af enkeltpersoner.

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

(62) Omkostningerne til udvikling af de planlagte interoperabilitetskomponenter under den nuværende flerårige finansielle ramme er lavere end det resterende beløb på budgettet til intelligente grænser i Europa-Parlamentets og Rådets forordning (EU) nr. 515/2014[61]. I medfør af artikel 5, stk. 5, litra b), i forordning (EU) nr. 515/2014 bør det beløb, der for øjeblikket er afsat til udvikling af IT-systemer til støtte for forvaltningen

[60] Europa-Parlamentets og Rådets forordning (EU) 2016/399 af 9. marts 2006 om en EU-kodeks for personers grænsepassage (Schengengrænsekodeks) (EUT L 77 af 23.3.2016, s. 1).

[61] 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).

af migrationsstrømme på tværs af de ydre grænser, følgelig omfordeles ved hjælp af denne forordning.

(63) For at supplere visse detaljerede tekniske aspekter af denne forordning bør beføjelsen til at vedtage retsakter i henhold til artikel 290 i traktaten om Den Europæiske Unions funktionsmåde uddelegeres til Kommissionen med henblik på profilerne for brugere af den europæiske søgeportal (ESP) og indholdet og formatet af svarene fra ESP. 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[62]. For at sikre lige deltagelse i udarbejdelsen af delegerede retsakter bør Europa-Parlamentet og Rådet navnlig modtage alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter bør have systematisk adgang til møder i de ekspertgrupper i Kommissionen, der beskæftiger sig med udarbejdelsen af delegerede retsakter.

(64) For at sikre at der opstilles ensartede betingelser for gennemførelsen af denne forordning, bør Kommissionen have gennemførelsesbeføjelser til at fastsætte detaljerede regler om: automatiske datakvalitetskontrolmekanismer, -procedurer og -indikatorer, udvikling af UMF-standarden, procedurer til bestemmelse af tilfælde af ens identiteter, driften af det centrale register for rapportering og statistik og en samarbejdsprocedure i tilfælde af sikkerhedshændelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011[63].

(65) Forordning (EU) 2016/794 finder anvendelse på Europols behandling af oplysninger med henblik på denne forordning.

(66) Denne forordning berører ikke anvendelsen af direktiv 2004/38/EF.

(67) Denne forordning udgør en udvikling af bestemmelser i Schengenreglerne.

(68) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om oprettelse af Det Europæiske Fællesskab, 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 til udbygning af Schengenreglerne, træffer Danmark afgørelse om, hvorvidt det vil gennemføre denne forordning i sin nationale lovgivning, jf. artikel 4 i protokollen.

(69) Denne forordning udgør en udvikling af bestemmelser i Schengenreglerne, som Det Forenede Kongerige ikke deltager i, jf. Rådets afgørelse 2000/365/EF[64]. Det Forenede Kongerige deltager derfor ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Det Forenede Kongerige.

(70) Denne forordning udgør en udvikling af bestemmelser i Schengenreglerne, som Irland ikke deltager i, jf. Rådets afgørelse 2002/192/EF[65]. Irland deltager derfor ikke i

---

62 http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.DAN.

63 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).

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

65 Rådets afgørelse 2002/192/EF af 28. februar 2002 om anmodningen fra Irland om at deltage i visse bestemmelser i Schengenreglerne (EFT L 64 af 7.3.2002, s. 20).

vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Irland.

(71) For så vidt angår Island og Norge udgør denne forordning en udvikling af 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[66], henhørende under det område, der er nævnt i artikel 1, litra A, B og G, i Rådets afgørelse 1999/437/EF om visse gennemførelsesbestemmelser til nævnte aftale[67].

(72) For så vidt angår Schweiz udgør denne forordning en udvikling af 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[68], henhørende under det område, der er nævnt i artikel 1, litra A, B og G, i afgørelse 1999/437/EF sammenholdt med artikel 3 i Rådets afgørelse 2008/146/EF[69].

(73) For så vidt angår Liechtenstein er denne forordning en udvikling af 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[70], henhørende under det område, der er nævnt i artikel 1, litra A, B og G, i afgørelse 1999/437/EF sammenholdt med artikel 3 i Rådets afgørelse 2011/350/EU[71].

(74) For så vidt angår Cypern udgør bestemmelserne vedrørende SIS og VIS bestemmelser, der bygger på Schengenreglerne eller på anden måde har tilknytning dertil, jf. artikel 3, stk. 2, i tiltrædelsesakten af 2003.

(75) For så vidt angår Bulgarien og Rumænien udgør bestemmelserne vedrørende SIS og VIS bestemmelser, der bygger på Schengenreglerne eller på anden måde har tilknytning dertil, jf. artikel 4, stk. 2, i tiltrædelsesakten af 2005 sammenholdt med Rådets afgørelse 2010/365/EU[72] og Rådets afgørelse (EU) 2017/1908[73].

(76) For så vidt angår Kroatien udgør bestemmelserne vedrørende SIS og VIS bestemmelser, der bygger på Schengenreglerne eller på anden måde har tilknytning dertil, jf. artikel 4, stk. 2, i tiltrædelsesakten af 2011, og bør sammenholdes med Rådets afgørelse (EU) 2017/733[74].

---

66 EFT L 176 af 10.7.1999, s. 36.
67 EFT L 176 af 10.7.1999, s. 31.
68 EUT L 53 af 27.2.2008, s. 52.
69 EUT L 53 af 27.2.2008, s. 1.
70 EUT L 160 af 18.6.2011, s. 21.
71 EUT L 160 af 18.6.2011, s. 19.
72 Rådets afgørelse 2010/365/EU af 29. juni 2010 om anvendelse af Schengenreglernes bestemmelser om Schengeninformationssystemet i Republikken Bulgarien og Rumænien (EUT L 166 af 1.7.2010, s. 17).
73 Rådets afgørelse (EU) 2017/1908 af 12 oktober 2017 om anvendelse af visse bestemmelser i Schengenreglerne om visuminformationssystemet i Republikken Bulgarien og Rumænien (EUT L 269 af 19.10.2017, s. 39).
74 Rådets afgørelse (EU) 2017/733 af 25. april 2017 om anvendelsen af bestemmelserne i Schengenreglerne om Schengeninformationssystemet i Kroatien (EUT L 108 af 26.4.2017, s. 31).

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

(78) For at denne forordning skal passe ind i den eksisterende juridiske ramme, bør forordning (EU) 2016/399, forordning (EU) 2017/2226, Rådets afgørelse 2008/633/RIA, forordning (EF) 767/2008 og Rådets afgørelse 2004/512/EF ændres i overensstemmelse hermed —

VEDTAGET DENNE FORORDNING:

KAPITEL I
Almindelige bestemmelser

Artikel 1
Genstand

1. Denne forordning fastsætter sammen med [forordning 2018/xx om interoperabilitet i politisamarbejde og retligt samarbejde, asyl og migration] en ramme, der skal sikre interoperabilitet mellem ind-og udrejsesystemet, visuminformationssystemet (VIS), [EU-systemet vedrørende rejseinformation og rejsetilladelse (ETIAS)], Eurodac og Schengeninformationssystemet (SIS) og [det europæiske informationssystem til udveksling af oplysninger fra strafferegistre vedrørende tredjelandsstatsborgere (ECRIS-TCN)], således at disse systemer og data kan supplere hinanden.

2. Rammen skal omfatte følgende interoperabilitetskomponenter:

   a) en europæisk søgeportal (ESP)

   b) en fælles biometrisk matchtjeneste (fælles BMS)

   c) et fælles identitetsregister

   d) en multiidentitetsdetektor (MID).

3. Denne forordning fastsætter også bestemmelser om datakvalitetskrav, om et universelt meddelelsesformat (UMF) og om et centralt register til rapportering og statistik (CRRS) og fastsætter ansvarsområderne for medlemsstaterne og Agenturet for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) med hensyn til udformning og drift af interoperabilitetskomponenterne.

4. Denne forordning tilpasser også procedurer og betingelser for adgangen for medlemsstaternes retshåndhævende myndigheder og Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) til ind- og udrejsesystemet, visuminformationssystemet (VIS), [EU-systemet vedrørende rejseinformation og rejsetilladelse (ETIAS)] og Eurodac med henblik på forebyggelse, opdagelse og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger, der henhører under deres kompetence.

Artikel 2
Mål om interoperabilitet

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

   a) at forbedre forvaltningen af de ydre grænser

   b) at bidrage til forebyggelse og bekæmpelse af irregulær migration

   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 og

   e) at bistå med at behandle ansøgninger om international beskyttelse.

2. Målene for at sikre interoperabilitet skal opnås ved at:

   a) sikre korrekt identifikation af personer

   b) bidrage til bekæmpelse af identitetssvig

   c) forbedre og harmonisere datakvalitetskravene i de respektive EU-informationssystemer

   d) lette den tekniske og operationelle gennemførelse i medlemsstaterne af eksisterende og fremtidige EU-informationssystemer

   e) styrke og forenkle de betingelser for datasikkerhed og databeskyttelse, der styrer de respektive EU-informationssystemer, og gøre dem mere ensartede

   f) effektivisere betingelserne for retshåndhævende myndigheders adgang til ind- og udrejsesystemet, VIS, [ETIAS] og Eurodac

   g) støtte formålet med ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS og [ECRIS-TCN-systemet].

Artikel 3
Anvendelsesområde

1. Denne forordning gælder for [ind- og udrejsesystemet], visuminformationssystemet (VIS), [det europæiske system vedrørende rejseinformation og rejsetilladelse (ETIAS)] og Schengeninformationssystemet (SIS).

2. Denne forordning gælder for personer, hvis personoplysninger må behandles i de EU-informationssystemer, der er nævnt i stk. 1.

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) "grænsekontrol": grænsekontrol som defineret i artikel 2, nr. 11, i forordning (EU) 2016/399

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

4) "tilsynsmyndigheder": den tilsynsmyndighed, der er oprettet i henhold til artikel 51, stk. 1, i forordning (EU) 2016/679, og den tilsynsmyndighed, der er oprettet i henhold til artikel 41, stk. 1, i direktiv (EU) 2016/680

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

6) "identifikation": fastlæggelse af en persons identitet via en databasesøgning på grundlag af flere datasæt (kontrol ved sammenligning af mange datasæt)

7) "tredjelandsstatsborger": en person, der ikke er unionsborger, jf. artikel 20, stk. 1, i traktaten, eller en statsløs person eller en person, hvis nationalitet er ukendt

8) "alfanumeriske data": data, der er angivet med bogstaver, tal, specialtegn, mellemrum og skilletegn

9) "identitetsdata": de data, som er omhandlet i artikel 27, stk. 3, litra a)-h)

10) "fingeraftryksdata": data om en persons fingeraftryk

11) "ansigtsbillede": digitale billeder af ansigtet

12) "biometriske data": fingeraftryksdata og/eller ansigtsbillede

13) "biometrisk skabelon": en matematisk gengivelse opnået ved at udlede træk fra biometriske data begrænset til de egenskaber, som er nødvendige for at foretage identifikationer og verifikationer

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

15) "rejsedokumentoplysninger": type, nummer og udstedelsesland for rejsedokumentet, udløbsdato for rejsedokumentets gyldighed og koden på tre bogstaver for det land, der udsteder rejsedokumentet

16) "rejsetilladelse": rejsetilladelse som defineret i artikel 3 i [ETIAS-forordningen]

17) "visum til kortvarigt ophold": visum som defineret i artikel 2, stk. 2, litra a), i forordning (EF) nr. 810/2009

18) "EU-informationssystemer": de store IT-systemer, som forvaltes af eu-LISA

19) "Europol-data": de personoplysninger, der forelægges Europol til de formål, der er omhandlet i artikel 18, stk. 2, litra a), i forordning (EU) 2016/794

20) "Interpol-databaser": Interpols database over stjålne og bortkomne rejsedokumenter og Interpols database over rejsedokumenter med tilknyttede notifikationer (TDAWN)

21) "match": et sammenfald, der fastslås ved at sammenligne to eller flere forekomster af personoplysninger, der er registreret eller ved at blive registreret i et informationssystem eller en database

22) "hit": bekræftelse af et eller flere match

23) "politimyndighed": "kompetent myndighed" som defineret i artikel 3, stk. 7, i direktiv 2016/680

24) "udpegede myndigheder": myndigheder udpeget af medlemsstaterne som omhandlet i artikel 29, stk. 1, i forordning (EU) 2017/2226, artikel 3, stk. 1, i

Rådets afgørelse 2008/633/RIA, [artikel 43 i ETIAS-forordningen] og [artikel 6 i Eurodac-forordningen]

25) "terrorhandling": en lovovertrædelse i henhold til national ret, der svarer til eller er ligestillet med en af de i direktiv (EU) 2017/541 omhandlede lovovertrædelser

26) "alvorlig strafbar handling": en lovovertrædelse, som svarer til eller er ligestillet med en af de i artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA omhandlede lovovertrædelser, hvis de i henhold til national ret kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år

27) "ind- og udrejsesystem": ind- og udrejsesystemet som omhandlet i forordning (EU) 2017/2226

28) "VIS": visuminformationssystemet som omhandlet i forordning (EF) nr. 767/2008

29) ["ETIAS": det europæiske system for rejseoplysninger og rejsetilladelser som omhandlet i ETIAS-forordningen]

30) "Eurodac": Eurodac som omhandlet i [Eurodac-forordningen]

31) "SIS": Schengeninformationssystemet som omhandlet [i SIS-forordningen inden for grænsekontrol, SIS-forordningen inden for retshåndhævelse og SIS-forordningen inden for ulovlig tilbagevenden]

32) ["ECRIS-TCN-systemet": det europæiske informationssystem vedrørende strafferegistre, der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer som omhandlet i forordningen om ECRIS-TCN-systemet]

33) "ESP": den europæiske søgeportal som omhandlet i artikel 6

34) "fælles BMS": den fælles biometriske matchtjeneste som omhandlet i artikel 15

35) "det fælles identitetsregister": det fælles identitetsregister som omhandlet i artikel 17

36) "MID": multiidentitetsdetektoren som omhandlet i artikel 25

37) "CRRS": det centrale register for rapportering og statistik som omhandlet i artikel 39.

Artikel 5
Ikke-forskelsbehandling

Behandling af personoplysninger i henhold til denne forordning må ikke medføre forskelsbehandling af en person på grund af køn, race eller etnisk oprindelse, religion eller tro, handicap, alder eller seksuel orientering. Den skal fuldt ud respektere den menneskelige værdighed og integritet. Der skal tages særligt hensyn til børn, ældre og personer med handicap.

KAPITEL II
Den europæiske søgeportal

Artikel 6
En europæisk søgeportal

1. Der oprettes en europæisk søgeportal (ESP) med henblik på at sikre, at medlemsstaternes myndigheder og EU-organerne har hurtig, problemfri, effektiv, systematisk og kontrolleret adgang til de EU-informationssystemer, Europol-data og Interpol-databaser, som de skal bruge til at udføre deres opgaver i overensstemmelse med deres adgangsret, og for at understøtte målene i ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN-systemet] og Europol-dataene.

2. ESP skal bestå af:

   a) en central infrastruktur, herunder en søgeportal, der muliggør samtidige søgninger i ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN-systemet] samt Europol-dataene og Interpol-databaserne

   b) en sikker kommunikationskanal mellem ESP, medlemsstaterne og de EU-organer, der har ret til at bruge ESP i overensstemmelse med EU-retten

   c) en sikker kommunikationsinfrastruktur mellem ESP og ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, det centrale SIS, [ECRIS-TCN-systemet], Europol-dataene og Interpol-databaserne samt mellem ESP og de centrale infrastrukturer i det fælles identitetsregister og multiidentitetsdetektoren.

3. eu-LISA skal udvikle og stå for den tekniske forvaltning af ESP.

Artikel 7
Brug af den europæiske søgeportal

1. Brugen af ESP er forbeholdt medlemsstaternes myndigheder og de EU-organer, der har adgang til ind- og udrejsesystemet, [ETIAS], VIS, SIS, Eurodac og [ECRIS-TCN-systemet], til det fælles identitetsregister og multiidentitetsdetektoren samt Europol-dataene og Interpol-databaserne i henhold til EU-retten eller national ret vedrørende en sådan adgang.

2. De myndigheder, der henvises til i stk. 1, bruger ESP til at søge efter data om personer eller deres rejsedokumenter i de centrale systemer i ind- og udrejsesystemet, VIS og [ETIAS] i overensstemmelse med deres adgangsret i henhold til EU-retten og national ret. De bruger også ESP til at foretage forespørgsler i det fælles identitetsregister i overensstemmelse med deres adgangsret i henhold til denne forordning, til de i artikel 20, 21 og 22 nævnte formål.

3. Medlemsstaternes myndigheder, der er nævnt i stk. 1, kan benytte ESP til at søge efter data om personer eller deres rejsedokumenter i det centrale SIS, der er nævnt i [SIS-forordningen inden for grænsekontrol og SIS-forordningen inden for retshåndhævelse]. Adgangen til det centrale SIS via ESP skal etableres gennem det nationale system (N.SIS) for hver medlemsstat, jf. [artikel 4, stk. 2, i SIS-forordningen inden for grænsekontrol og i SIS-forordningen inden for retshåndhævelse].

4. EU-organerne skal bruge ESP til at søge efter data om personer eller deres rejsedokumenter i det centrale SIS.

5. De myndigheder, der henvises til i stk. 1, kan benytte ESP til at søge efter data om personer eller deres rejsedokumenter i Interpol-databaserne 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 skal eu-LISA oprette en profil for hver kategori af brugere af ESP i overensstemmelse med de tekniske detaljer og adgangsrettigheder, som er nævnt i stk. 2, herunder, i overensstemmelse med EU-retten og national ret:

   a) de dataområder, som skal bruges til at forespørge

   b) EU-informationssystemerne, Europol-dataene, Interpol-databaserne, der skal og kan konsulteres, og som skal give et svar til brugeren og

   c) de data, der gives i hvert svar.

2. Kommissionen vedtager delegerede retsakter som omhandlet i artikel 63 for at specificere de tekniske oplysninger om de i stk. 1 nævnte profiler over for de brugere af ESP, som er nævnt i artikel 7, stk. 1, i overensstemmelse med deres adgangsret.

Artikel 9
Forespørgsler

1. Brugerne af ESP foretager en forespørgsel ved at indføre data i ESP i overensstemmelse med deres brugerprofil og adgangsrettigheder. Hvis der er foretaget en forespørgsel, skal ESP foretage forespørgsler samtidigt ved hjælp af de data, som er indlæst af brugere af ESP, ind- og udrejsesystemet, [ETIAS], VIS, SIS, Eurodac, [ECRIS-TCN-systemet] og det fælles identitetsregister samt Europol-dataene og Interpol-databaserne.

2. De dataområder, der anvendes til at foretage en forespørgsel via ESP, skal svare til de dataområder vedrørende personer eller rejsedokumenter, der kan anvendes til at foretage forespørgsler i de forskellige EU-informationssystemer, Europol-dataene og Interpol-databaserne i overensstemmelse med de retlige instrumenter, der regulerer dem.

3. eu-LISA gennemfører et grænsefladekontroldokument baseret på UMF som omhandlet i artikel 38 for ESP.

4. Ind- og udrejsesystemet, [ETIAS], VIS, SIS, Eurodac, [ECRIS-TCN-systemet], det fælles identitetsregister og multiidentitetsdetektoren samt Europol-dataene og Interpol-databaserne giver de data, de indeholder som følge af forespørgslen i ESP.

5. Ved en forespørgsel i Interpol-databaserne sikrer udformningen af ESP, at de data, der anvendes af brugeren af ESP til at foretage en forespørgsel, ikke deles med ejerne af Interpol-dataene.

6. Svaret til brugerne af ESP er unikt og indeholder alle de oplysninger, som brugeren har adgang til i henhold til EU-retten. Om nødvendigt angives det i svaret fra ESP, hvilket informationssystem eller database dataene kommer fra.

7. Kommissionen vedtager en delegeret retsakt, jf. artikel 63 for at præcisere form og indhold af svarene fra ESP.

Artikel 10
Opbevaring af logfiler

1. Med forbehold af [artikel 46 i forordningen om ind- og udrejsesystemet], artikel 34 i forordning (EF) nr. 767/2008, [artikel 59 i forslaget om ETIAS] og artikel 12 og 18 i SIS-forordningen inden for grænsekontrol fører eu-LISA logfiler over alle databehandlinger i ESP. Disse logfiler omfatter især følgende:

   a) medlemsstatens myndighed og den enkelte bruger af ESP, herunder den anvendte ESP-profil som omhandlet i artikel 8

   b) dato og klokkeslæt for forespørgslen

   c) de EU-informationssystemer og Interpol-databaser, der foretages forespørgsler i

   d) i overensstemmelse med nationale regler eller, når det er relevant, forordning (EU) nr. 45/2001 referenceangivelsen for den person, der har foretaget forespørgslen.

2. Logfilerne må kun bruges til overvågning af databeskyttelsen, herunder til at kontrollere grundlaget for en forespørgsel og lovligheden af databehandlingen, og til at garantere datasikkerheden, jf. artikel 42. Logfilerne skal beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter oprettelsen, medmindre de er nødvendige til kontrolprocedurer, som allerede er indledt.

Artikel 11
Alternative procedurer, hvis det er teknisk umuligt at anvende den europæiske søgeportal

1. Hvis det er teknisk umuligt at anvende ESP til at foretage forespørgsler i et eller flere af de EU-informationssystemer, der er omhandlet i artikel 9, stk. 1, eller i det fælles identitetsregister på grund af en fejl i ESP, underretter eu-LISA brugerne af ESP om dette.

2. Hvis det er teknisk umuligt at anvende ESP til at foretage forespørgsler i et eller flere af de EU-informationssystemer, der er omhandlet i artikel 9, stk. 1, eller det fælles identitetsregister på grund af en fejl i den nationale infrastruktur i en medlemsstat, underretter den pågældende medlemsstats kompetente myndighed eu-LISA og Kommissionen om dette.

3. I begge scenarier og indtil den tekniske fejl er rettet, finder forpligtelsen i artikel 7, stk. 2 og 4, ikke anvendelse, og medlemsstaterne kan få adgang til de informationssystemer, der er nævnt i artikel 9, stk. 1, eller det fælles identitetsregister direkte ved hjælp deres respektive nationale ensartede grænseflader eller nationale kommunikationsinfrastruktur.

KAPITEL III
Den fælles biometriske matchtjeneste

Artikel 12
Fælles biometrisk matchtjeneste

1. Der oprettes en fælles biometrisk matchtjeneste (fælles BMS), der lagrer biometriske skabeloner og gør det muligt at foretage forespørgsler med biometriske data på tværs af flere EU-informationssystemer, med henblik på at understøtte det fælles identitetsregister og multiidentitetsdetektoren og målene for ind- og udrejsesystemet, VIS, Eurodac, SIS og [ECRIS-TCN-systemet].

2. Den fælles BMS består af:

   a) en central infrastruktur, herunder en søgemaskine og lagring af data som omhandlet i artikel 13

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

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

Artikel 13
Data lagret i den fælles biometriske matchtjeneste

1. Den fælles BMS lagrer de biometriske skabeloner, som indhentes fra følgende biometriske data:

   a) de data, der er omhandlet i artikel 16, stk. 1, litra d), og artikel 17, stk. 1, litra b) og c), i forordning (EU) 2017/2226

   b) de data, der er omhandlet i artikel 9, stk. 6, i forordning (EF) nr. 767/2008

   c) [de data, der er omhandlet i artikel 20, stk. 2, litra w) og x), i SIS-forordningen inden for grænsekontrol

   d) de data, der er omhandlet i artikel 20, stk. 3, litra w) og x), i SIS-forordningen inden for retshåndhævelse

   e) de data, der er omhandlet i artikel 4, stk. 3, litra t) og u), i SIS-forordningen inden for ulovlig tilbagesendelse]

   f) [de data, der er omhandlet i artikel 13, litra a), i Eurodac-forordningen]

   g) [de data, der er omhandlet i artikel 5, stk. 1, litra b), og artikel 5, stk. 2, i ECRIS-TCN-forordningen.]

2. Den fælles BMS indeholder i hver biometrisk skabelon en henvisning til de informationssystemer, hvor de pågældende biometriske data er lagret.

3. Biometriske skabeloner må kun indlæses i den fælles BMS efter en automatisk kvalitetskontrol af de biometriske data, der føjes til et af informationssystemerne, som udføres af den fælles BMS for at sikre, at en minimumsstandard for datakvalitet er opfyldt.

4. Lagringen af de data, der er omhandlet i stk. 1, skal opfylde de kvalitetsstandarder, der er omhandlet i artikel 37, stk. 2.

Artikel 14
Søgning efter biometriske data med den fælles biometriske matchtjeneste

Til at søge efter de biometriske data, som er lagret i det fælles identitetsregister og SIS, anvender det fælles identitetsregister og SIS biometriske skabeloner, der er lagret i den fælles BMS. Forespørgsler med biometriske data finder sted i overensstemmelse med de formål, der er fastsat i denne forordning og i forordningen om ind- og udrejsesystemet, VIS, SIS, Eurodac-forordningen [SIS-forordningerne] og [ECRIS-TCN-forordningen].

Artikel 15
Datalagring i den fælles biometriske matchtjeneste

De data, der er omhandlet i artikel 13, lagres i den fælles BMS, så længe de pågældende biometriske data lagres i det fælles identitetsregister eller SIS.

Artikel 16
Logfiler

1. Med forbehold af [artikel 46 i forordningen om ind- og udrejsesystemet], artikel 34 forordning (EF) nr. 767/2008 og [artikel 12 og 18 i SIS-forordningen inden for retshåndhævelse] fører eu-LISA logfiler over alle databehandlinger i den fælles BMS. Disse logfiler omfatter navnlig:
   a) historikken vedrørende oprettelse og lagring af biometriske skabeloner
   b) en henvisning til de EU-informationssystemer, hvori der foretages forespørgsler med de biometriske skabeloner, der er lagret i den fælles BMS
   c) dato og klokkeslæt for forespørgslen
   d) typen af biometriske data, der bruges til at foretage forespørgslen
   e) forespørgslens længde
   f) resultaterne af forespørgslen og dato og tidspunkt for resultatet
   g) i overensstemmelse med nationale regler eller, når det er relevant, forordning (EU) nr. 45/2001 referenceangivelsen for den person, der har foretaget forespørgslen.
2. Logfilerne må kun bruges til overvågning af databeskyttelse, herunder til at kontrollere grundlaget for en forespørgsel og lovligheden af databehandlingen, og til at garantere datasikkerheden, jf. artikel 42. Logfilerne skal beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter oprettelsen, medmindre de er nødvendige til kontrolprocedurer, som allerede er indledt. De i stk. 1, litra a), omhandlede logfiler slettes, når dataene slettes.

KAPITEL IV
Det fælles identitetsregister

Artikel 17
Det fælles identitetsregister

1. Der oprettes et fælles identitetsregister, hvori der oprettes en individuel fil for hver person, der registreres i ind- og udrejsesystemet, VIS, [ETIAS], Eurodac eller [ECRIS-TCN-systemet], som indeholder de data, der er omhandlet i artikel 18, med henblik på at lette og bistå en korrekt identifikation af personer registreret i ind- og udrejsesystemet, VIS, [ETIAS], Eurodac og [ECRIS-TCN-systemet], støtte driften af multiidentitetsdetektoren og lette og effektivisere de retshåndhævende myndigheders adgang til informationssystemer på EU-niveau, der ikke vedrører retshåndhævelse, når det er nødvendigt for at forebygge, efterforske, opdage eller retsforfølge alvorlige strafbare handlinger.

2. Det fælles identitetsregister består af:

   a) en central infrastruktur, der erstatter de centrale systemer i henholdsvis ind- og udrejsesystemet, VIS, [ETIAS], Eurodac og [ECRIS-TCN-systemet], og som lagrer de data, der er omhandlet i artikel 18

   b) en sikker kommunikationskanal mellem det fælles identitetsregister, medlemsstaterne og de EU-organer, der er berettiget til at benytte den europæiske søgeportal (ESP) i overensstemmelse med EU-retten

   c) en sikker kommunikationsinfrastruktur mellem det fælles identitetsregister og ind- og udrejsesystemet, [ETIAS], VIS, Eurodac og ECRIS-TCN-systemet] samt med de centrale infrastrukturer i ESP, den fælles BMS og multiidentitetsdetektoren.

3. eu-LISA udvikler og står for den tekniske forvaltning af det fælles identitetsregister

Artikel 18
Data i det fælles identitetsregister

1. Det fælles identitetsregister lagrer følgende data – logisk opdelt – alt efter hvilket informationssystem dataene hidrører fra:

   a) de data, der er omhandlet i [artikel 16, stk. 1, litra a)-d), og artikel 17, stk. 1, litra a)-c), i forordningen om ind- og udrejsesystemet]

   b) de data, der er omhandlet i artikel 9, stk. 4, litra a)-c), stk. 5 og 6, i forordning (EF) nr. 767/2008

   c) [de data, der er omhandlet i artikel 15, stk. 2, litra a)-e), i [ETIAS-forordningen]

   d) – (ikke relevant)

   e) – (ikke relevant)

2. For hvert af de i stk. 1 omhandlede datasæt indeholder det fælles identitetsregister en henvisning til de informationssystemer, som indeholder dataene.

3. Lagringen af de data, der er omhandlet i stk. 1, skal opfylde de kvalitetsstandarder, der er omhandlet i artikel 37, stk. 2.

Artikel 19

Tilføjelse, ændring og sletning af data i det fælles identitetsregister

1. Hvis der tilføjes, ændres eller slettes data i ind- og udrejsesystemet, VIS og [ETIAS], tilføjes, ændres eller slettes de data, der er omhandlet i artikel 18, som er lagret i det fælles identitetsregister, automatisk.

2. Hvis multiidentitetsdetektoren opretter et hvidt eller rødt link, jf. artikel 32 og 33, mellem data fra to eller flere af de EU-informationssystemer, der udgør det fælles identitetsregister, i stedet for at skabe en ny, individuel fil, tilføjer det fælles identitetsregister de nye data til den individuelle fil for de sammenkædede data.

Artikel 20

Adgang til det fælles identitetsregister med henblik på identifikation

1. Hvis en medlemsstats politimyndighed har beføjelse hertil i medfør af nationale lovgivningsmæssige foranstaltninger som omhandlet i stk. 2, kan den udelukkende med henblik på at identificere en person foretage en forespørgsel i det fælles identitetsregister med den pågældende persons biometriske data, som er indsamlet ved en identitetskontrol.

   Hvis forespørgslen viser, at dataene for den pågældende person er lagret i det fælles identitetsregister, har medlemsstatens myndighed adgang til at konsultere de data, der er omhandlet i artikel 18, stk. 1.

   Hvis de biometriske data for den pågældende person ikke kan anvendes, eller hvis forespørgslen med de pågældende data slår fejl, foretages søgningen med personens identitetsdata kombineret med oplysningerne i rejsedokumenterne eller med identitetsdata fra denne person.

2. De medlemsstater, som ønsker at benytte sig af muligheden i denne artikel, vedtager nationale lovgivningsmæssige foranstaltninger. Sådanne lovgivningsmæssige foranstaltninger skal indeholde det præcise formål med identitetskontrollen i overensstemmelse med 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.

Artikel 21

Adgang til det fælles identitetsregister til påvisning af flere identiteter

1. Hvis en forespørgsel fra det fælles identitetsregister resulterer i et gult link, jf. artikel 28, stk. 4, har den ansvarlige myndighed for verifikation af forskellige identiteter, der fastslås som omhandlet i artikel 29, udelukkende med henblik på denne verifikation adgang til de identitetsdata, som er lagret i det fælles identitetsregister, og som findes i de forskellige informationssystemer, der er knyttet til et gult link.

2. Hvis en forespørgsel i det fælles identitetsregister resulterer i et rødt link, jf. artikel 32, har de myndigheder, der er omhandlet i artikel 26, stk. 2, udelukkende med henblik på bekæmpelse af identitetssvig adgang til de identitetsdata, som er lagret i det fælles identitetsregister, og som findes i de forskellige informationssystemer, der er knyttet til et rødt link.

Artikel 22

Forespørgsler i det fælles identitetsregister til retshåndhævelsesformål

1. Med henblik på at forebygge, opdage og efterforske terrorhandlinger eller andre alvorlige strafbare handlinger i en specifik sag og for at indhente oplysninger om, hvorvidt der findes data om en bestemt person i ind- og udrejsesystemet, VIS og [ETIAS], kan medlemsstaternes udpegede myndigheder og Europol konsultere det fælles identitetsregister.

2. Medlemsstaternes udpegede myndigheder og Europol har ikke ret til at konsultere data, der tilhører [ECRIS-TCN-systemet], når de konsulterer det fælles identitetsregister til de formål, der fremgår af stk. 1.

3. Hvis det fælles identitetsregister som svar på en forespørgsel angiver, at der findes data om personen i ind- og udrejsesystemet, VIS og [ETIAS], skal det fælles identitetsregister give medlemsstaternes udpegede myndigheder og Europol svar i form af en henvisning til, hvilke af informationssystemerne der indeholder matchende data som omhandlet i artikel 18, stk. 2. Alle svar fra det fælles identitetsregister skal udformes således, at datasikkerheden ikke bringes i fare.

4. Fuld adgang til dataene i EU-informationssystemerne med henblik på at forebygge, opdage og efterforske terrorhandlinger eller andre alvorlige strafbare handlinger er fortsat underlagt betingelserne og procedurerne i de respektive lovgivningsmæssige instrumenter, der regulerer denne adgang.

Artikel 23

Lagring af data i det fælles identitetsregister

1. De i artikel 18, stk. 1 og 2, omhandlede data slettes fra det fælles identitetsregister i overensstemmelse med bestemmelserne i [forordningen om ind- og udrejsesystemet], VIS-forordningen og [ETIAS-forordningen].

2. Den enkelte fil lagres i det fælles identitetsregister, så længe de tilsvarende data er lagret i mindst ét af de informationssystemer, hvis data er indeholdt i det fælles identitetsregister. Hvis der oprettes et link, berører dette ikke lagringsperioden for hvert af elementerne i de sammenkædede data.

Artikel 24

Logfiler

1. Med forbehold af [artikel 46 i forordningen om ind- og udrejsesystemet], artikel 34 i forordning (EF) nr. 767/2008 og [artikel 59 i forslaget om ETIAS] fører eu-LISA logfiler over alle databehandlinger i det fælles identitetsregister, jf. stk. 2, 3 og 4.

2. Hvad angår adgang til det fælles identitetsregister i henhold til artikel 20, fører eu-LISA logfiler over alle databehandlinger i det fælles identitetsregister. Disse logfiler omfatter navnlig følgende:

   a) formålet med adgangen til den bruger, der foretager en forespørgsel via det fælles identitetsregister

   b) dato og klokkeslæt for forespørgslen

   c) typen af data, der bruges til at foretage forespørgslen

   d) resultaterne af forespørgslen

e) i overensstemmelse med nationale regler eller forordning (EU) 2016/794 eller, når dette er relevant, forordning (EU) nr. 45/2001, referenceangivelsen på den person, der har foretaget forespørgslen.

3. Hvad angår adgang til det fælles identitetsregister i henhold til artikel 21, fører eu-LISA logfiler over alle databehandlinger i det fælles identitetsregister. Disse logfiler omfatter navnlig følgende:

a) formålet med adgangen til den bruger, der foretager en forespørgsel via det fælles identitetsregister

b) dato og klokkeslæt for forespørgslen

c) hvis det er relevant, de data, der bruges til at foretage forespørgslen

d) hvis det er relevant, resultaterne af forespørgslen

e) i overensstemmelse med nationale regler eller forordning (EU) 2016/794 eller, når det er relevant, forordning (EU) nr. 45/2001, referenceangivelsen på den person, der har foretaget forespørgslen.

4. Hvad angår adgang til det fælles identitetsregister i henhold til artikel 22, fører eu-LISA logfiler over alle databehandlinger i det fælles identitetsregister. Disse logfiler omfatter navnlig følgende:

a) henvisningen til den nationale fil

b) dato og klokkeslæt for forespørgslen

c) typen af data, der bruges til at foretage forespørgslen

d) resultaterne af forespørgslen

e) navnet på den myndighed, der konsulterer det fælles identitetsregister

f) i overensstemmelse med nationale regler eller forordning (EU) 2016/794 eller, når det er relevant, forordning (EU) nr. 45/2001, referenceangivelsen på den embedsmand, der har foretaget forespørgslen og på den embedsmand, der bestilte forespørgslen.

Logfilerne vedrørende denne adgang kontrolleres regelmæssigt af den kompetente tilsynsmyndighed, der er udpeget som fastsat i artikel 51 forordning (EU) 2016/679 eller som fastsat i artikel 41 direktiv 2016/680, med intervaller på højst seks måneder, for at kontrollere, at de procedurer og betingelser, der er fastsat i artikel 22, stk. 1 til 3, er opfyldt.

5. Hver medlemsstat fører logfiler over spørgsmål fra medarbejdere, der er behørigt bemyndiget til at anvende det fælles identitetsregister i medfør af artikel 20, 21 og 22.

6. De logfiler, der er omhandlet i stk. 1-5, må kun bruges til overvågning af databeskyttelsen, herunder til at kontrollere grundlaget for en forespørgsel og lovligheden af databehandlingen, og til at garantere datasikkerheden, jf. artikel 42. De skal beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter oprettelsen, medmindre de er nødvendige til kontrolprocedurer, som allerede er indledt.

7. eu-LISA lagrer de logfiler, der er relateret til historikken for de data, der lagres i de enkelte filer, til de formål, der er fastsat i stk. 6. De logfiler, der vedrører historikken for de lagrede data, slettes, når dataene slettes.

KAPITEL V
Multiidentitetsdetektoren

Artikel 25
Multiidentitetsdetektoren

1. Der oprettes en multiidentitetsdetektor (MID), der opretter og lagrer links mellem data i de EU-informationssystemer, der indgår i det fælles identitetsregister og SIS og dermed påviser flere identiteter, med det dobbelte formål at lette identitetskontrollen og bekæmpe identitetssvig, med henblik på at støtte det fælles identitetsregisters funktioner og målene for ind- og udrejsesystemet, VIS, [ETIAS], Eurodac, SIS og [ECRIS-TCN-systemet].

2. MID skal bestå af:

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

   b) en sikker kommunikationsinfrastruktur til at forbinde MID med SIS og de centrale infrastrukturer i den europæiske søgeportal og det fælles identitetsregister.

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

Artikel 26
Adgang til multiidentitetsdetektoren

1. For så vidt angår den manuelle identitetsverifikation som omhandlet i artikel 29 gives følgende adgang til de data, der er omhandlet i artikel 34, og som er lagret i MID:

   a) grænsemyndigheder ved oprettelse eller ajourføring af en individuel fil, jf. artikel 14 i [forordningen om ind- og udrejsesystemet]

   b) de kompetente myndigheder, der er omhandlet i artikel 6, stk. 1 og 2, i forordning (EF) nr. 767/2008, i forbindelse med udarbejdelse eller ajourføring af en ansøgningsfil i VIS, jf. artikel 8 i forordning (EF) nr. 767/2008

   c) [den centrale ETIAS-enhed og de nationale ETIAS-enheder, når de foretager den vurdering, der er omhandlet i artikel 20 og 22 i ETIAS-forordningen]

   d) – (ikke relevant)

   e) SIRENE-kontoret i den medlemsstat, som har oprettet en [SIS-indberetning i overensstemmelse med SIS-forordningen inden for grænsekontrol]

   f) – (ikke relevant).

2. Medlemsstaternes myndigheder og de EU-organer, der har adgang til mindst ét EU-informationssystem, der indgår i det fælles identitetsregister eller SIS, skal have adgang til de data, der er omhandlet i artikel 34, litra a) og b), vedrørende eventuelle røde links som omhandlet i artikel 32.

Artikel 27
Påvisning af flere identiteter

1. Der foretages en påvisning af flere identiteter i det fælles identitetsregister og SIS, hvis:

   a) der oprettes en individuel fil, eller denne ajourføres i [ind- og udrejsesystemet, jf. artikel 14 i forordningen om ind- og udrejsesystemet]

   b) der oprettes en ansøgningsfil, eller denne ajourføres i VIS, jf. artikel 8 forordning (EF) nr. 767/2008

   c) [der oprettes en ansøgningsfil, eller denne ajourføres i ETIAS, jf. artikel 17 ETIAS-forordningen]

   d) – (ikke relevant)

   e) [der oprettes en indberetning om en person i SIS, eller denne ajourføres, jf. kapitel V i SIS-forordningen inden for grænsekontrol]

   f) – (ikke relevant).

2. Hvis data i et informationssystem som omhandlet i stk. 1 indeholder biometriske data, anvender det fælles identitetsregister og det centrale SIS den fælles biometriske matchtjeneste (fælles BMS) til at påvise flere identiteter. Den fælles BMS sammenholder de biometriske skabeloner fra eventuelle nye biometriske data med de biometriske skabeloner, der allerede er indeholdt i den fælles BMS, til at verificere, om data tilhørende den samme tredjelandsstatsborger allerede er lagret i det fælles identitetsregister eller i det centrale SIS.

3. Ud over den proces, der er omhandlet i stk. 2, anvender det fælles identitetsregister og det centrale SIS den europæiske søgeportal til at søge efter data lagret i det fælles identitetsregister og det centrale SIS ved hjælp af følgende data:

   a) efternavn, fornavn(e) fødselsdato, køn og nationalitet(er) som omhandlet i artikel 16, stk. 1, litra a), i [forordningen om ind- og udrejsesystemet]

   b) efternavn, fornavn(e) fødselsdato, køn og nationalitet(er) som omhandlet i artikel 9, stk. 4, litra a), i forordning (EF) nr. 767/2008

   c) [efternavn) fornavn(e) fødenavn fødselsdato, fødested, køn og nationalitet(er) som omhandlet i artikel 15, stk. 2, i ETIAS-forordningen]

   d) – (ikke relevant)

   e) [efternavn(e) fornavn(e) navn(e) ved fødslen, tidligere anvendte navne og aliasser, fødselsdato, fødested, nationalitet(er) og køn som omhandlet i artikel 20, stk. 2, i SIS-forordningen inden for grænsekontrol]

   f) – (ikke relevant)

   g) – (ikke relevant)

   h) – (ikke relevant).

4. Påvisning af flere identiteter foretages kun for at sammenligne data i ét informationssystem med data i andre informationssystemer.

Artikel 28
Resultater af påvisningen af flere identiteter

1. Hvis de forespørgsler, der er omhandlet i artikel 27, stk. 2, og 3, ikke giver noget hit, fortsætter de procedurer, der er omhandlet i artikel 27, stk. 1, i overensstemmelse med de respektive forordninger, der regulerer dem.

2. Hvis forespørgslen i artikel 27, stk. 2 og 3, giver ét eller flere hit(s), opretter det fælles identitetsregister og, hvis det er relevant, SIS et link mellem de data, som er anvendt til at foretage forespørgslen, og de data, der udløste et hit.

   Hvis der gives flere hits, oprettes et link mellem alle de data, der udløste hittet. Hvis der allerede var et link til dataene, udvides det eksisterende link til de data, der blev anvendt til at foretage forespørgslen.

3. Hvis den forespørgsel, der er omhandlet i artikel 27, stk. 2 eller 3, giver et eller flere hit, og identitetsdataene for de tilknyttede filer er identiske eller ensartede, oprettes et hvidt link, jf. artikel 33.

4. Hvis den forespørgsel, der er omhandlet i artikel 27, stk. 2 eller 3, giver et eller flere hit, og identitetsdataene for de tilknyttede filer ikke kan betragtes som ensartede, oprettes et gult link, jf. artikel 30, og proceduren i artikel 29 finder anvendelse.

5. Kommissionen fastsætter procedurerne for at fastslå, hvornår identitetsdata kan betragtes som identiske eller ensartede, i gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 64, stk. 2.

6. Links opbevares i identitetsbekræftelsesfilen som omhandlet i artikel 34.

Kommissionen fastsætter de tekniske regler for oprettelse af links mellem data fra forskellige informationssystemer i gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 64, stk. 2.

Artikel 29
Manuel verifikation af forskellige identiteter

1. Med forbehold af stk. 2, er den ansvarlige myndighed for verifikation af de forskellige identiteter:

   a) grænsemyndigheden for hit, der forekom i forbindelse med oprettelse eller ajourføring af en individuel fil i [ind- og udrejsesystemet, jf. artikel 14 i forordningen om ind- og udrejsesystemet]

   b) de kompetente myndigheder som omhandlet i artikel 6, stk. 1 og 2, i forordning 767/2008 for hit, der forekom i forbindelse med oprettelse eller ajourføring af en ansøgningsfil i VIS, jf. artikel 8 i forordning (EF) nr. 767/2008

   c) [den centrale ETIAS-enhed og de nationale ETIAS-enheder for hit, der forekom som omhandlet i artikel 18, 20 og 22 i ETIAS-forordningen]

   d) – (ikke relevant)

   e) SIRENE-kontorerne i medlemsstaten for hit, der forekom i forbindelse med oprettelse af en SIS-indberetning i overensstemmelse med [SIS-forordningerne inden for grænsekontrol]

   f) – (ikke relevant).

Multiidentitetsdetektoren viser, hvilken myndighed der er ansvarlig for verifikationen af forskellige identiteter i identitetsverifikationsfilen.

2. Den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter i identitetsbekræftelsesfilen, er SIRENE-kontoret i den medlemsstat, som oprettede indberetningen, der indeholdt et link til data i:

   a) en indberetning om personer, der begæres anholdt med henblik på overgivelse eller udlevering, jf. artikel 26 i [SIS-forordningen inden for retshåndhævelse]

   b) en indberetning om forsvundne eller sårbare personer, jf. artikel 32 i [SIS-forordningen inden for retshåndhævelse]

   c) en indberetning om personer, der eftersøges med henblik på at yde bistand i forbindelse med retsforfølgning, jf. artikel 34 i [SIS-forordningen inden for retshåndhævelse]

   d) [i en indberetning om tilbagesendelse i overensstemmelse med SIS-forordningen inden for ulovlig tilbagesendelse]

   e) i en indberetning om personer med henblik på diskret kontrol, undersøgelseskontrol eller målrettet kontrol som omhandlet i artikel 36 i [SIS-forordningen inden for retshåndhævelse]

   f) i en indberetning om ukendte eftersøgte personer med henblik på identifikation i overensstemmelse med national ret og søgning med biometriske data som omhandlet i artikel 40 i [SIS-forordningen inden for retshåndhævelse].

3. Uden at dette berører stk. 4, har den myndighed, der er for verifikationen af de forskellige identiteter adgang til de relevante data, der er indeholdt i de relevante identitetsbekræftelsesfiler, og til de sammenkædede identitetsdata i det fælles identitetsregister, og, hvis det er relevant, i SIS, og vurderer de forskellige identiteter og ajourfører linket som fastsat i artikel 31, 32 og 33 og føjer det straks til identitetsbekræftelsesfilen.

4. Hvis den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter i identitetsbekræftelsesfilen er den grænsemyndighed, der opretter eller ajourfører en individuel fil i ind- og udrejsesystemet, jf. artikel 14 i forordningen om ind- og udrejsesystemet, og hvis der fremkommer et gult link, foretager grænsemyndigheden supplerende verifikation som en del af kontrollen i anden linje. Under denne kontrol i anden linje har grænsemyndigheden adgang til de relevante data i den relevante identitetsbekræftelsesfil og adgang til de forskellige identiteter og opdaterer linket som fastsat i artikel 31 til 33 og føjer det straks til identitetsbekræftelsesfilen.

5. Hvis der opnås mere end ét link, vurderer den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, hvert link særskilt.

6. Hvis data, der giver et hit, allerede er sammenkædet, tager den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, hensyn til de eksisterende links ved vurderingen af oprettelsen af nye links.

Artikel 30
Gult link

1. Et link mellem data fra to eller flere informationssystemer skal klassificeres som gule i følgende tilfælde:

a) de sammenkædede data har samme biometriske data, men forskellige identitetsdata, og der er ikke foregået nogen manuel verifikation af de forskellige identiteter

b) de sammenkædede data har forskellige identitetsdata, og der er ikke foregået nogen manuel verifikation af de forskellige identiteter.

2. Hvis et link er klassificeret som gult, jf. stk. 1, finder proceduren i artikel 29 anvendelse.

Artikel 31
Grønt link

1. Et link mellem data fra to eller flere informationssystemer skal klassificeres som grønt, hvis de sammenkædede data ikke har samme biometriske data, men har ens identitetsdata, og den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, har konkluderet, at det henviser til to forskellige personer.

2. Når det fælles identitetsregister eller SIS forespørges, og der findes et grønt link mellem to eller flere af de informationssystemer, der udgør det fælles identitetsregister, eller med SIS, angiver multiidentitetsdetektoren, at identitetsdataene for de sammenkædede data ikke svarer til den samme person. I svaret fra det forespurgte informationssystem angives udelukkende data for den person, hvis data blev anvendt til forespørgslen, uden at det udløser et hit i forhold til de data, der er omfattet af det grønne link.

Artikel 32
Rødt link

1. Et link mellem data fra to eller flere informationssystemer klassificeres som rødt i følgende tilfælde:

a) de sammenkædede data har samme biometriske data, men forskellige identitetsdata, og den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, har konkluderet, at de henviser ulovligt til den samme person

b) de sammenkædede data har ensartede identitetsoplysninger, og den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, har konkluderet, at de henviser ulovligt til den samme person.

2. Hvis det fælles identitetsregister eller SIS forespørges, og der findes et rødt link mellem to eller flere af de informationssystemer, der udgør det fælles identitetsregister, eller med SIS, viser multiidentitetsdetektoren de data, der er omhandlet i artikel 34. Opfølgning på et rødt link finder sted i overensstemmelse med EU-retten og national ret.

3. Hvis der oprettes et rødt link mellem data fra ind- og udrejsesystemet, VIS, Eurodac, [ETIAS] eller [ECRIS-TCN-systemet], ajourføres den individuelle fil, der er lagret i det fælles identitetsregister, jf. artikel 19, stk. 1.

4. Med forbehold af bestemmelserne vedrørende behandlingen af indberetninger i SIS, der er omhandlet i [SIS-forordningerne inden for grænsekontrol, retshåndhævelse og ulovlig tilbagesendelse] og med forbehold af de begrænsninger, der er nødvendige

for at beskytte den offentlige sikkerhed og den offentlige orden, forebygge kriminalitet og sikre, at eventuelle nationale efterforskninger ikke bringes i fare, underretter den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, hvis der oprettes et rødt link, den pågældende person om, at der er flere ulovlige identiteter.

5. Hvis der oprettes et rødt link, henviser den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, til de myndigheder, der er ansvarlige for de sammenkædede data.

Artikel 33
Hvidt link

1. Et link mellem data fra to eller flere informationssystemer klassificeres som hvidt i følgende tilfælde:

   a) de sammenkædede data har samme biometriske data og de samme eller ensartede identitetsdata

   b) de sammenkædede data har samme eller ensartede identitetsdata, og mindst ét af informationssystemerne har ingen biometriske data for den pågældende person

   c) de sammenkædede data har samme biometriske data, men forskellige identitetsdata, og den myndighed, der er ansvarlig for verifikationen af forskellige identiteter, har konkluderet, at de henviser til den samme person, der lovligt har forskellige identitetsdata.

2. Hvis det fælles identitetsregister eller SIS forespørges, og der findes et hvidt link mellem et eller flere af de informationssystemer, der udgør det fælles identitetsregister eller med SIS, angiver multiidentitetsdetektoren, at de sammenkædede data svarer til den samme person. I svaret fra de forespurgte informationssystemer angives alle de sammenkædede data for den pågældende person, hvis det er relevant, hvilket giver et hit i forhold til de data, som er omfattet af det hvide link, hvis den myndighed, der foretager forespørgslen, har adgang til de sammenkædede data i henhold til EU-retten eller national ret.

3. Hvis der oprettes et hvidt link mellem data fra ind- og udrejsesystemet, VIS, [ETIAS], Eurodac eller [ECRIS-TCN-systemet], ajourføres den enkelte fil, der er lagret i det fælles identitetsregister som fastsat i artikel 19, stk. 1.

4. Med forbehold af bestemmelserne vedrørende håndtering af indberetninger i SIS som omhandlet i [SIS-forordningerne inden for grænsekontrol, retshåndhævelse og ulovlig tilbagesendelse] underretter den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter, hvis der oprettes et hvidt link efter en manuel verifikation af flere identiteter, den pågældende person om, at der er en uoverensstemmelse mellem dennes personoplysninger mellem systemerne og henviser til den ansvarlige myndighed for de sammenkædede data.

Artikel 34
Identitetsbekræftelsesfil

Identitetsbekræftelsesfilen indeholder følgende data:

   a) links, herunder en beskrivelse af disse i form af farver som omhandlet i artikel 30 og 33

b) en henvisning til de informationssystemer, hvis data er sammenkædede

c) et enkelt identifikationsnummer, som gør det muligt at hente data fra informationssystemer med tilsvarende sammenkædede filer

d) hvis det er relevant, den myndighed, der er ansvarlig for verifikationen af de forskellige identiteter.

Artikel 35
Lagring af data i multiidentitetsdetektoren

Identitetsbekræftelsesfiler og data, herunder links, lagres kun i multiidentitetsdetektoren (MID), så længe de sammenkædede data er lagret i to eller flere EU-informationssystemer.

Artikel 36
Opbevaring af logfiler

1. eu-LISA fører logfiler over alle databehandlinger i multiidentitetsdetektoren. Disse logfiler omfatter navnlig:

   a) formålet med brugerens adgang og dennes adgangsrettigheder

   b) dato og klokkeslæt for forespørgslen

   c) typen af data, der anvendes til at foretage forespørgslen eller forespørgslerne

   d) henvisning til de sammenkædede data

   e) historikken for identitetsbekræftelsesfilen

   f) referenceangivelsen på den person, der har foretaget forespørgslen.

2. Hver medlemsstat fører logfiler over de medarbejdere, som er behørigt bemyndiget til at anvende multiidentitetsdetektoren.

3. Logfilerne må kun bruges til overvågning af databeskyttelsen, herunder til at kontrollere grundlaget for en forespørgsel og lovligheden af databehandlingen, og til at garantere datasikkerheden, jf. artikel 42. Logfilerne skal beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes et år efter oprettelsen, medmindre de er nødvendige til kontrolprocedurer, som allerede er indledt. Logfilerne vedrørende historikken for identitetsbekræftelsesfilen slettes, så snart dataene i identitetsbekræftelsesfilen slettes.

KAPITEL VI
Foranstaltninger til støtte for interoperabilitet

Artikel 37
Datakvalitet

1. eu-LISA indfører automatiske mekanismer og procedurer for datakvalitetskontrol af de data, som er lagret i ind- og udrejsesystemet, ETIAS, VIS, SIS, den fælles biometriske matchtjeneste (fælles BMS), det fælles identitetsregister og multiidentitetsdetektoren (MID).

2. eu-LISA indfører fælles datakvalitetsindikatorer og minimumskvalitetsstandarder for lagring af data i ind- og udrejsesystemet, [ETIAS], VIS, SIS, den fælles BMS, det fælles identitetsregister 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.

4. De nærmere detaljer om de automatiske mekanismer til og procedurer for datakvalitetskontrol og de fælles datakvalitetsindikatorer og minimumskvalitetsstandarderne for lagring af data i ind- og udrejsesystemet, [ETIAS], VIS, SIS, den fælles BMS, det fælles identitetsregister og MID, navnlig vedrørende biometriske data, fastsættes i gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 64, stk. 2.

5. Et år efter indførelsen af de automatiske mekanismer til og procedurer for datakvalitetskontrol og de fælles datakvalitetsindikatorer 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 blev konstateret i evalueringsrapporten, og aflægger rapport 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 og Den Europæiske Unions Agentur for Grundlæggende Rettigheder, som er oprettet ved Rådets forordning (EF) nr. 168/2007[75].

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/eller organisationer inden for retlige og indre anliggender.

2. UMF-standarden anvendes i forbindelse med udviklingen af ind- og udrejsesystemet, [ETIAS], den europæiske søgeportal, det fælles identitetsregister, MID og, når det er relevant, i forbindelse med eu-LISA's eller et andet EU-organs udvikling af nye modeller til informationsudveksling og informationssystemer inden for retlige og indre anliggender.

3. Det kan overvejes at gennemføre UMF-standarden i VIS, SIS og i eventuelle eksisterende eller nye modeller til grænseoverskridende informationsudveksling og informationssystemer inden for retlige og indre anliggender, som er udviklet af medlemsstaterne eller associerede lande.

4. Kommissionen vedtager en gennemførelsesretsakt til fastlæggelse og udvikling af UMF-standarden i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 64, stk. 2.

[75] 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).

Artikel 39
Centralt register til rapportering og statistik

1. Der oprettes et centralt register til rapportering og statistik (CRRS) med henblik på at støtte målene for ind- og udrejsesystemet, VIS, [ETIAS] og SIS og til at generere statistiske data og analytisk rapportering på tværs af systemerne til politiske, operationelle og datakvalitetsmæssige formål.

2. eu-LISA opretter, gennemfører og hoster CRRS på sine tekniske websteder, der indeholder de data, der omhandlet i [artikel 63 i forordningen om ind- og udrejsesystemet], artikel 17 i forordning (EF) nr. 767/2008, [artikel 73 i ETIAS-forordningen] og [artikel 54 i SIS-forordningen inden for grænsekontrol], der holdes logisk adskilt. Dataene i CRRS giver ikke mulighed for identifikation af enkeltpersoner. Der skal gives adgang til registret via en sikret adgang gennem kommunikationsnetværket TESTA (Trans-European Services for Telematics between Administrations), idet der anvendes adgangskontrol og særlige brugerprofiler udelukkende med henblik på rapportering og statistik, til de myndigheder, der er omhandlet i [artikel 63 i forordningen om ind- og udrejsesystemet], artikel 17 forordning (EF) nr. 767/2008, artikel 73 i ETIAS-forordningen] og [artikel 54 i SIS-forordningen inden for grænsekontrol].

3. eu-LISA anonymiserer dataene og registrerer disse anonyme data i CRRS. Anonymiseringen af dataene foregår automatisk.

4. CRRS består af:

   a) en central infrastruktur bestående af et dataregister, der gør det muligt at anonymisere data

   b) en sikker kommunikationsinfrastruktur, der forbinder CRRS til ind- og udrejsesystemet [ETIAS], VIS og SIS samt de centrale infrastrukturer i den fælles BMS, det fælles identitetsregister og MID.

5. Kommissionen fastsætter de nærmere regler for driften af CRRS, herunder specifikke sikkerhedsforanstaltninger for behandling af personoplysninger som omhandlet i stk. 2 og 3 og de sikkerhedsregler, der gælder for registret, ved hjælp af gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 64, stk. 2.

KAPITEL VII
Databeskyttelse

Artikel 40
Registeransvarlig

1. For så vidt angår behandlingen af data i den fælles biometriske matchtjeneste (fælles BMS), betragtes de af medlemsstaternes myndigheder, der er registeransvarlige for VIS, ind- og udrejsesystemet og SIS, også som registeransvarlige i henhold til artikel 4, stk. 7, i forordning (EU) 2016/679 i forhold til de biometriske skabeloner fra de data, der er omhandlet i artikel 13, som de indlæser i de respektive systemer, og de er ansvarlige for behandlingen af de biometriske skabeloner i den fælles BMS.

2. For så vidt angår behandling af data i det fælles identitetsregister betragtes de af medlemsstaternes myndigheder, der er registeransvarlige for VIS, ind- og udrejsesystemet og [ETIAS], også som registeransvarlige i henhold til artikel 4, stk. 7, i forordning (EU) 2016/679 i forhold til de data, der er omhandlet i artikel 18, som de indlæser i de enkelte systemer, og de er ansvarlige for behandlingen af de pågældende personoplysninger i det fælles identitetsregister.

3. For så vidt angår behandling af data i multiidentitetsdetektoren:

   a) betragtes Det Europæiske Agentur for Grænse- og Kystbevogtning som registeransvarlig, jf. artikel 2, litra b), i forordning (EF) nr. 45/2001 i forhold til den behandling af personoplysninger, der foretages af den centrale ETIAS-enhed

   b) betragtes de af medlemsstaternes myndigheder, der tilføjer eller ændrer data i identitetsbekræftelsesfilen, også som registeransvarlige, jf. artikel 4, stk. 7, i forordning (EU) 2016/679, og de er ansvarlige for behandlingen af personoplysninger i multiidentitetsdetektoren.

Artikel 41
Databehandler

For så vidt angår behandlingen af personoplysninger i det fælles identitetsregister betragtes eu-LISA som databehandler, jf. artikel 2, litra e), i forordning (EF) nr. 45/2001.

Artikel 42
Behandlingssikkerhed

1. Både eu-LISA og medlemsstaternes myndigheder sørger for sikkerheden i forbindelse med den behandling af personoplysninger, der finder sted i henhold til anvendelsen af denne forordning. eu-LISA, [den centrale ETIAS-enhed] og medlemsstaternes myndigheder samarbejder om sikkerhedsrelaterede opgaver.

2. Uden at det berører artikel 22 i forordning (EF) nr. 45/2001, 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 forretningskontinuitets- og katastrofeberedskabsplan, med henblik på at:

   a) beskytte data fysisk, bl.a. ved at udarbejde beredskabsplaner for beskyttelse af kritisk infrastruktur

   b) forhindre, at uautoriserede personer læser, kopierer, ændrer eller fjerner datamedier

   c) forhindre uautoriseret indlæsning af data samt uautoriseret læsning, ændring eller sletning af registrerede personoplysninger

   d) forhindre uautoriseret behandling af data samt uautoriseret kopiering, ændring eller sletning af data

   e) sikre, at autoriserede personer i forhold til at få adgang til interoperabilitetskomponenterne kun får adgang til de data, der er omfattet af deres adgangstilladelse, ved hjælp af individuelle brugeridentiteter og fortrolige adgangsmetoder

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

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

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

i) kontrollere effektiviteten af sikkerhedsforanstaltningerne i dette stykke og træffe de nødvendige organisatoriske foranstaltninger vedrørende intern kontrol for at sikre overholdelsen af denne forordning.

4. Medlemsstaterne træffer foranstaltninger svarende til dem, der er nævnt i stk. 3, for så vidt angår sikkerhed, når myndigheder, der har adgangsret til en hvilken som helst af interoperabilitetskomponenterne, behandler personoplysninger.

Artikel 43
Fortrolighed vedrørende SIS-data

1. Hver medlemsstat anvender i overensstemmelse med national lovgivning sine egne regler for tavshedspligt eller tilsvarende fortrolighedskrav i forbindelse med alle personer og organer, der skal arbejde med SIS-data, som de har adgang til via en af interoperabilitetskomponenterne. Denne pligt fortsætter med at bestå, efter at de pågældende personer er fratrådt deres stilling, eller det pågældende organs virksomhed er ophørt.

2. eu-LISA anvender passende regler for tavshedspligt eller tilsvarende fortrolighedskrav i forhold til alt personale, der skal arbejde med SIS-data, efter standarder svarende til dem, der er fastsat i stk. 1, jf. dog artikel 17 i vedtægten for tjenestemænd i Den Europæiske Union og ansættelsesvilkårene for Unionens øvrige ansatte. Denne pligt fortsætter med at bestå, efter at de pågældende personer er fratrådt deres stilling, eller deres virksomhed er ophørt.

Artikel 44
Sikkerhedshændelser

1. Enhver hændelse, der har eller kan have indvirkning på sikkerheden i interoperabilitetskomponenterne og kan forårsage skade eller tab af data, som er lagret deri, anses for at være en sikkerhedshændelse, især når der er sket uautoriseret adgang til data, eller når tilgængeligheden, integriteten og fortroligheden af data er eller kan være blevet sat over styr.

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

3. Uden at det berører anmeldelsen og kommunikationen af et brud på persondatasikkerheden, jf. artikel 33 i forordning (EU) 2016/679, artikel 30 i direktiv (EU) 2016/680 eller begge, underretter medlemsstaterne Kommissionen, eu-LISA og Den Europæiske Tilsynsførende for Databeskyttelse om sikkerhedshændelser. I tilfælde af en sikkerhedshændelse, der vedrører interoperabilitetskomponenternes

centrale infrastruktur, underretter eu-LISA Kommissionen og Den Europæiske Tilsynsførende for Databeskyttelse.

4. Der gives oplysninger om en sikkerhedshændelse, der har eller kan have indvirkning på driften af interoperabilitetskomponenterne eller på tilgængeligheden, integriteten og fortroligheden af dataene, til medlemsstaterne, og der rapporteres herom i overensstemmelse med den hændelsesstyringsplan, som eu-LISA skal udforme.

5. De berørte medlemsstater og eu-LISA samarbejder i tilfælde af en sikkerhedshændelse. Kommissionen fastsætter retningslinjerne for dette samarbejde ved hjælp af gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 64, stk. 2.

Artikel 45
Egenkontrol

Medlemsstaterne og de relevante EU-organer 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 samarbejder i nødvendigt omfang med den nationale tilsynsmyndighed.

De registeransvarlige, jf. artikel 40, træffer de nødvendige foranstaltninger for at overvåge, at databehandlingen sker i henhold til denne forordning, herunder hyppig kontrol af logfiler, og samarbejder, når det er nødvendigt, med tilsynsmyndighederne som omhandlet i artikel 49 og 50.

Artikel 46
Ret til oplysninger

1. Uden at dette berører retten til oplysninger, jf. artikel 11 og 12 i forordning (EF) 45/2001 og artikel 13 og 14 i forordning (EU) 2016/679, underrettes personer, hvis data er lagret i den fælles biometriske matchtjeneste, det fælles identitetsregister eller multiidentitetsdetektoren, af den myndighed, der indsamler deres data, på det tidspunkt, hvor deres data indsamles, om behandlingen af personoplysninger med henblik på denne forordning, herunder om identitets- og kontaktoplysninger for de respektive registeransvarlige, og om procedurerne for udøvelse af deres ret til indsigt, berigtigelse og sletning, samt om kontaktoplysninger for Den Europæiske Tilsynsførende for Databeskyttelse og den nationale tilsynsmyndighed i den medlemsstat, der er ansvarlig for indsamlingen af data.

2. Personer, hvis data registreres i ind- og udrejsesystemet, VIS eller [ETIAS], underrettes om behandlingen af data med henblik på denne forordning i henhold til stk. 1, når:

   a) [der oprettes en individuel fil, eller denne ajourføres i ind- og udrejsesystemet, jf. artikel 14 i forordningen om ind- og udrejsesystemet]

   b) der oprettes en ansøgningsfil, eller denne ajourføres i VIS, jf. artikel 8 forordning (EF) nr. 767/2008

   c) [der oprettes en ansøgningsfil, eller denne ajourføres i ETIAS, jf. artikel 17 ETIAS-forordningen]

   d) – (ikke relevant)

   e) – (ikke relevant).

Artikel 47
Ret til indsigt, berigtigelse og sletning

1. For at kunne udøve sin ret i henhold til artikel 13, 14, 15 og 16 i forordning (EF) 45/2001 og artikel 15, 16, 17 og 18 i forordning (EU) 2016/679 har enhver person ret til at henvende sig til den medlemsstat, der er ansvarlig for den manuelle verifikation af forskellige identiteter, eller enhver anden medlemsstat, der undersøger og besvarer anmodningen.

2. Den ansvarlige medlemsstat for manuel verifikation af forskellige identiteter, jf. artikel 29, eller den medlemsstat, hvortil anmodningen er rettet, besvarer sådanne anmodninger senest 45 dage efter modtagelsen heraf.

3. Hvis en anmodning om berigtigelse eller sletning af personoplysninger indgives til en anden medlemsstat end den ansvarlige medlemsstat, kontakter den medlemsstat, som anmodningen er indgivet til, myndighederne i den ansvarlige medlemsstat inden for syv dage, og den ansvarlige medlemsstat kontrollerer rigtigheden af dataene og lovligheden af databehandlingen senest 30 dage efter denne henvendelse.

4. Hvis det efter en undersøgelse konstateres, at de data, der er lagret i multiidentitetsdetektoren (MID), er ukorrekte eller ulovligt registreret, berigtiger eller sletter den ansvarlige medlemsstat eller i givet fald den medlemsstat, som anmodningen er indgivet til, disse data.

5. Hvis data i MID ændres af den ansvarlige medlemsstat i løbet af gyldighedsperioden, gennemfører den ansvarlige medlemsstat behandlingen i artikel 27 og, hvis det er relevant artikel 29 for at fastslå, om de ændrede data skal sammenkædes. Såfremt behandlingen ikke resulterer i et hit, sletter den ansvarlige medlemsstat eller i givet fald den medlemsstat, som anmodningen er indgivet til, dataene i identitetsbekræftelsesfilen. Hvis den automatiserede behandling resulterer i et eller flere hit, opretter eller ajourfører den ansvarlige medlemsstat det relevante link i overensstemmelse med de relevante bestemmelser i denne forordning.

6. Hvis den ansvarlige medlemsstat eller i givet fald den medlemsstat, som anmodningen er indgivet til, ikke er enig i, at de data, som er lagret i MID, er faktuelt ukorrekte eller er registreret ulovligt, træffer denne medlemsstat en administrativ afgørelse og forklarer straks skriftligt den pågældende person, hvorfor den ikke er villig til at berigtige eller slette dataene om vedkommende.

7. Denne afgørelse skal også give den berørte person oplysninger om muligheden for at anfægte afgørelsen vedrørende den i stk. 3 omhandlede anmodning, og, hvis det er relevant, om, hvordan der kan klages over afgørelsen til de kompetente myndigheder eller afgørelsen kan prøves ved domstolene, samt om eventuel bistand hertil, herunder fra de kompetente nationale tilsynsmyndigheder.

8. En anmodning indgivet i henhold til stk. 3 skal indeholde de nødvendige oplysninger til at identificere den pågældende person. De pågældende oplysninger må udelukkende anvendes til at muliggøre udøvelsen af de rettigheder, der er nævnt i stk. 3, og skal slettes umiddelbart efter.

9. Den ansvarlige medlemsstat eller i givet fald den medlemsstat, som anmodningen er indgivet til, registrerer i et skriftligt dokument, at der er indgivet en anmodning som omhandlet i stk. 3, samt hvordan den blev håndteret, og stiller straks dokumentet til rådighed for de kompetente nationale tilsynsmyndigheder for databeskyttelse.

Artikel 48
Videregivelse af personoplysninger til tredjelande, internationale organisationer og private parter

Personoplysninger, der lagres eller tilgås af interoperabilitetskomponenterne, må ikke overføres til eller stilles til rådighed for et tredjeland, en international organisation eller en privat part med undtagelse af overførsler til Interpol med henblik på den automatiserede behandling, der er omhandlet i [artikel 18, stk. 2, litra b) og m), i ETIAS-forordningen] eller artikel 8, stk. 2, i forordning (EU) 2016/399. Sådanne overførsler af personoplysninger til Interpol skal være i overensstemmelse med bestemmelserne i artikel 9 i forordning (EF) nr. 45/2001 og kapitel V i forordning (EU) 2016/679.

Artikel 49
Den nationale tilsynsmyndigheds tilsyn

1. Den eller de nationale tilsynsmyndighed(er), som er udpeget i henhold til artikel 49 i forordning (EU) 2016/679, sikrer, at de ansvarlige nationale myndigheder mindst hvert fjerde år foretager en revision af behandlingen af data i overensstemmelse med relevante internationale revisionsstandarder.

2. Medlemsstaterne sikrer, at deres tilsynsmyndighed har tilstrækkelige ressourcer til at udføre de opgaver, som er tillagt den i henhold til denne forordning.

Artikel 50
Tilsyn 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 behandling af personoplysninger i overensstemmelse med relevante internationale revisionsstandarder. Europa-Parlamentet, Rådet, eu-LISA, Kommissionen og medlemsstaterne tilsendes en rapport om denne revision. eu-LISA skal have mulighed for at fremsætte bemærkninger, inden rapporterne vedtages.

Artikel 51
Samarbejde mellem de nationale tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse

1. Den Europæiske Tilsynsførende for Databeskyttelse handler i tæt samarbejde med de nationale tilsynsmyndigheder med hensyn til specifikke spørgsmål, der kræver nationalt engagement, især hvis Den Europæiske Tilsynsførende for Databeskyttelse eller en national tilsynsmyndighed finder store forskelle mellem medlemsstaternes praksis eller potentielt ulovlige overførsler ved hjælp af kommunikationskanalerne for interoperabilitetskomponenterne eller i forbindelse med spørgsmål rejst af en eller flere nationale tilsynsmyndigheder om gennemførelsen og fortolkningen af denne forordning.

2. I de i stk. 1 nævnte tilfælde sikres det koordinerede tilsyn som fastsat i artikel 62 i forordning (EU) XXXX / 2018 [revideret forordning (EF) nr. 45/2001].

KAPITEL VIII
Ansvarsområder

Artikel 52
eu-LISA's ansvarsområder i 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 lokaliteter og leverer de funktionaliteter, der er fastsat i denne forordning, i overensstemmelse med betingelserne for sikkerhed, tilgængelighed, kvalitet og hastighed, jf. artikel 53, stk. 1.

3. eu-LISA er ansvarlig for udviklingen af interoperabilitetskomponenterne, for eventuelle tilpasninger, der kræves for at skabe interoperabilitet mellem de centrale systemer i ind- og udrejsesystemet, VIS, [ETIAS], SIS og Eurodac og [ECRIS-TCN-systemet] og den europæiske søgeportal, den fælles biometriske matchtjeneste, det fælles identitetsregister og multiidentitetsdetektoren.

   eu-LISA fastlægger udformningen af interoperabilitetskomponenternes fysiske struktur, herunder deres kommunikationsinfrastruktur og de tekniske specifikationer og deres udvikling, hvad angår den centrale infrastruktur og sikker kommunikationsinfrastruktur, der vedtages af bestyrelsen, med forbehold af en gunstig udtalelse fra Kommissionen. eu-LISA gennemfører også de nødvendige tilpasninger af ind- og udrejsesystemet, [ETIAS], SIS eller VIS som følge af skabelsen af interoperabilitet og som fastsat i denne forordning.

   eu-LISA udvikler og implementerer interoperabilitetskomponenterne så hurtigt 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 6, artikel 37, stk. 4, artikel 38, stk. 4, artikel 39, stk. 5, og artikel 44, stk. 5.

   Udviklingsarbejdet omfatter udarbejdelse og gennemførelse af de tekniske specifikationer, afprøvning og samlet projektkoordinering.

4. I udformnings- og udviklingsfasen nedsættes et programstyringsråd bestående af højst 10 medlemmer. Udvalget skal bestå af syv medlemmer udpeget af eu-LISA's bestyrelse blandt sine medlemmer eller suppleanter, formanden for den rådgivende gruppe for interoperabilitet, der er omhandlet i artikel 65, 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 af de medlemsstater, der i henhold til EU-retten er fuldt ud bundet af retsakterne om udvikling, oprettelse, drift og brug af alle de store it-systemer, der forvaltes af eu-LISA, 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 bestyrelsen om fremskridtene i projektet. 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 skal indeholde regler om:

   a) formandskab

   b) mødesteder

   c) forberedelse af møder

   d) eksperters adgang til møderne

   e) kommunikationsplan, der sikrer fuld information af fraværende medlemmer af bestyrelsen.

   Formandskabet varetages af en medlemsstat, der i henhold til EU-retten er fuldt ud bundet af retsakterne om udvikling, oprettelse, drift og brug af alle de store it-systemer, der forvaltes af eu-LISA.

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

   Den rådgivende interoperabilitetsgruppe, der er nævnt i artikel 65, 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 53
eu-LISA's forpligtelser efter idriftsættelsen

1. Efter idriftsættelsen af hver interoperabilitetskomponent er eu-LISA ansvarlig for den tekniske forvaltning af den centrale infrastruktur og de nationale ensartede grænseflader. I samarbejde med medlemsstaterne sikrer det den til enhver tid bedste disponible teknologi på grundlag af en cost-benefit-analyse. eu-LISA er også ansvarligt for den tekniske forvaltning af kommunikationsinfrastrukturen, der er omhandlet i artikel 6, 12, 17, 25 og 39.

   Den tekniske forvaltning af interoperabilitetskomponenterne omfatter alle de opgaver, der er nødvendige for, at interoperabilitetskomponenterne kan fungere døgnet rundt alle ugens syv dage i henhold til denne forordning, navnlig 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.

2. eu-LISA anvender passende regler for tavshedspligt eller tilsvarende fortrolighedskrav i forbindelse med alle medarbejdere, der skal arbejde med data lagret i interoperabilitetskomponenterne, jf. dog artikel 17 i tjenestemandsvedtægten. Denne pligt består fortsat, når de pågældende medarbejdere er fratrådt deres stilling, eller deres virksomhed er ophørt.

3. eu-LISA udvikler og vedligeholder en mekanisme til og procedurer for kvalitetskontrol af de data, der er lagret i den fælles biometriske matchtjeneste og det fælles identitetsregister, jf. artikel 37.

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

Artikel 54
Medlemsstaternes ansvar

1. Hver medlemsstat er ansvarlig for:

   a) forbindelsen til kommunikationsinfrastrukturen i den europæiske søgeportal (ESP) og det fælles identitetsregister

   b) integration af de eksisterende nationale systemer og infrastrukturer med ESP, den fælles biometriske matchtjeneste, det fælles identitetsregister og multiidentitetsdetektoren

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

   d) forvaltning af og ordninger for adgangsretten for behørigt bemyndigede medarbejdere og behørigt bemyndigede medarbejdere i de kompetente nationale myndigheder til ESP, det fælles identitetsregister og multiidentitetsdetektoren i overensstemmelse med denne forordning og oprettelse og regelmæssig ajourføring af en liste over disse medarbejdere og deres profiler

   e) vedtagelse af de lovgivningsmæssige foranstaltninger, der er omhandlet i artikel 20, stk. 3, for at få adgang til det fælles identitetsregister i identifikationsøjemed

   f) den manuelle verifikation af forskellige identiteter, der er omhandlet i artikel 29

   g) gennemførelse af datakvalitetskravene i EU's informationssystemer og i interoperabilitetskomponenterne

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

2. Hver medlemsstat forbinder de udpegede myndigheder, der er omhandlet i artikel 4, stk. 24, til det fælles identitetsregister.

Artikel 55
Den centrale ETIAS-enheds ansvar

Den centrale ETIAS-enhed er ansvarlig for:

   a) den manuelle verifikation af forskellige identiteter, der er omhandlet i artikel 29

   b) påvisning af flere identiteter blandt de data, der er lagret i VIS, Eurodac og SIS, jf. artikel 59.

KAPITEL IX
Ændringer af andre EU-instrumenter

Artikel 55a
Ændringer af forordning (EU) 2016/399

I forordning (EU) 2016/399 foretages følgende ændringer:

I artikel 8 i forordning (EU) 2016/399 indsættes som stk. 4a:

"4a. Hvis konsultationen af de relevante databaser i forbindelse med ind- eller udrejse, herunder multiidentitetsdetektoren via den europæiske søgeportal, der er omhandlet i henholdsvis [artikel 4, stk. 36 og 33, i forordning 2018/xx om interoperabilitet], resulterer i et gult link, eller der registreres et rødt link, henvises den person, der kontrolleres, til kontrol i anden linje.

Grænsevagten i anden linje konsulterer multiidentitetsdetektoren sammen med det fælles identitetsregister som omhandlet i [artikel 4, stk. 35, i forordning 2018/XX om interoperabilitet] eller Schengeninformationssystemet eller begge for at vurdere forskellene i de sammenkædede identiteter og foretager eventuel yderligere verifikation for at træffe en beslutning om status af og farven på linket samt for at træffe afgørelse om den pågældende persons indrejse eller nægtelse af indrejse.

Som fastsat i [artikel 59, stk. 1, i forordning nr. 2018/XX] gælder dette stykke kun fra idriftsættelsen af multiidentitetsdetektoren."

Artikel 55b
Ændringer af forordning (EU) 2017/2226

I forordning (EU) 2017/2226 foretages følgende ændringer:

1) I artikel 1 indsættes følgende stykke:

"1a. Ved at lagre identitetsdata, rejsedokumenter og biometriske data i det fælles identitetsregister oprettet ved [artikel 17 i forordning 2018/XX om interoperabilitet] bidrager ind- og udrejsesystemet til at fremme og bistå med en korrekt identifikation af personer, der er registreret i ind- og udrejsesystemet på de betingelser og med henblik på de ultimative målsætninger, som er omhandlet i [artikel 20] i nævnte forordning."

2) I artikel 3 indsættes som stk. 21a:

"Det fælles identitetsregister": det fælles identitetsregister som defineret i [artikel 4, nr. 35, i forordning 2018/XX om interoperabilitet]

3) Artikel 3, stk. 1, nr. 22, affattes således:

"(22)"Data fra ind- og udrejsesystemet": alle data lagret i ind- og udrejsesystemets centrale system og i det fælles identitetsregister, jf. artikel 14 og artikel 16 til 20.

4) I artikel 3 indsættes som nr. 22a:

"(22a) "identitetsdata": de data, som er omhandlet i artikel 16, stk. 1, litra a)"

5) I artikel 6, stk. 1, indsættes følgende litra:

"j) sikre korrekt identifikation af personer."

6) Artikel 7, stk. 1, litra a), affattes således:

"a) det fælles identitetsregister som omhandlet i [artikel 17, stk. 2, litra a), i forordning 2018/XX] om interoperabilitet]

aa) et centralt system (ind- og udrejsesystemets centrale system)"

7) Artikel 7, stk. 1, litra f), affattes således:

"f) en sikker kommunikationsinfrastruktur mellem ind- og udrejsesystemets centrale system og de centrale infrastrukturer i den europæiske søgeportal oprettet ved [artikel 6 i forordning 2018/XX om interoperabilitet], den fælles biometriske matchtjeneste oprettet ved [artikel 12 i forordning 2018/XX om interoperabilitet], det fælles

identitetsregister oprettet ved [artikel 17 i forordning 2018/XX om interoperabilitet] og multiidentitetsdetektoren oprettet ved [artikel 25 i forordning 2018/XX om interoperabilitet]".

8) I artikel 7 indsættes følgende stykke:

"1a. Det fælles identitetsregister indeholder de data, der er omhandlet i artikel 16, stk. 1, litra a)-d), og artikel 17, stk. 1, litra a)-c), og de resterende data i ind- og udrejsesystemet lagres i ind- og udrejsesystemets centrale system.

9) I artikel 9 indsættes følgende stykke:

"3. Adgang til konsultation af de data i ind- og udrejsesystemet, som er lagret i det fælles identitetsregister, er udelukkende forbeholdt behørigt bemyndigede medarbejdere ved de nationale myndigheder i hver enkelt medlemsstat og de behørigt bemyndigede medarbejdere i de EU-organer, der er kompetente med hensyn til de formål, der er fastsat i [artikel 20 og artikel 21 forordning 2018/XX om interoperabilitet]. Denne adgang begrænses i det omfang, det er nødvendigt for udførelsen af de nationale myndigheders og EU-organers opgaver i overensstemmelse med disse formål, og skal stå i forhold til de tilstræbte mål."

10) I artikel 21, stk. 1, erstattes "ind- og udrejsesystemets centrale system", begge gange udtrykket optræder, med "ind- og udrejsesystemets centrale system eller det fælles identitetsregister".

11) I artikel 21, stk. 2, erstattes "både ind- og udrejsesystemets centrale system og i den nationale ensartede grænseflade" af ordene "både i ind- og udrejsesystemets centrale system og det fælles identitetsregister på den ene side og i den nationale ensartede grænseflade på den anden side".

12) I artikel 21, stk. 2, erstattes ordene "registreres i ind- og udrejsesystemets centrale system" af ordene "registreres i ind- og udrejsesystemets centrale system og det fælles identitetsregister".

13) I artikel 32 indsættes som stk. 1a:

"1a. I tilfælde, hvor de udpegede myndigheder har foretaget en forespørgsel til det fælles identitetsregister, jf. [artikel 22 i forordning 2018/XX om interoperabilitet], kan de få adgang til ind- og udrejsesystemet med henblik på konsultation, hvor det modtagne svar som omhandlet i stk. 3 i [artikel 22 i forordning 2018/XX om interoperabilitet] viser, at der er lagret data i ind- og udrejsesystemet."

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

"2. Adgang til ind- og udrejsesystemet som et værktøj til identifikation af en ukendt mistænkt eller gerningsmand eller et formodet offer for en terrorhandling eller anden alvorlig strafbar handling er kun tilladt, når der er foretaget en forespørgsel i det fælles identitetsregister, jf. [artikel 22 forordning 2018/XX om interoperabilitet], og alle de betingelser, der er anført i stk. 1 og stk. 1a, er opfyldt.

Denne yderligere betingelse gælder dog ikke i hastende tilfælde, hvor der er behov for at forhindre en overhængende fare for en persons liv, hvis denne person har tilknytning til en terrorhandling eller en anden alvorlig strafbar handling. Disse rimelige grunde indgår i den elektroniske eller skriftlige anmodning, der sendes af driftsenheden i den udpegede myndighed til det centrale adgangspunkt."

15) Artikel 32, stk. 4, udgår.

16) I artikel 33 indsættes som stk. 1a:

"1a. I tilfælde, hvor Europol har foretaget en forespørgsel i det fælles identitetsregister, jf. [artikel 22 i forordning 2018/XX om interoperabilitet], kan Europol få adgang til ind- og udrejsesystemet med henblik på konsultation, hvis de modtagne svar som omhandlet i [artikel 22,]stk. 3[, i forordning 2018/XX om interoperabilitet] viser, at der er lagret data i ind- og udrejsesystemet."

17) Artikel 33, stk. 3, affattes således:

"Betingelserne i artikel 32, stk. 3 og 5, finder tilsvarende anvendelse"

18) I artikel 34, stk. 1 og 2, erstattes "i ind- og udrejsesystemets centrale system" af "i henholdsvis det fælles identitetsregister og ind- og udrejsesystemets centrale system".

19) 19) I artikel 34, stk. 5, erstattes "fra ind- og udrejsesystemets centrale system" af "fra ind- og udrejsesystemets centrale system og fra det fælles identitetsregister".

20) Artikel 35, stk. 7, affattes således:

"Ind- og udrejsesystemets centrale system og det fælles identitetsregister skal straks underrette alle medlemsstaterne om sletning af data i ind- og udrejsesystemet eller det fælles identitetsregister og, når det er relevant, fjerne dem fra listen over identificerede personer, jf. artikel 12, stk. 3."

21) I artikel 36 erstattes "i ind- og udrejsesystemets centrale system" af "i ind- og udrejsesystemets centrale system og i det fælles identitetsregister".

22) I artikel 37, stk. 1, erstattes "udvikling af ind- og udrejsesystemets centrale system" af "udvikling af ind- og udrejsesystemets centrale system og det fælles identitetsregister".

23) I artikel 37, stk. 3, første afsnit, erstattes "ind- og udrejsesystemets centrale system" første og tredje gang dette forekommer, af "ind- og udrejsesystemets centrale system og det fælles identitetsregister".

24) I artikel 46, stk. 1, indsættes følgende som litra f):

"f) hvis det er relevant, en henvisning til anvendelsen af den europæiske søgeportal til forespørgsler i ind- og udrejsesystemet som omhandlet i [artikel 7, stk. 2, i forordning 2018/XX om interoperabilitet]."

25) Artikel 63, stk. 2, affattes således:

"2. "Med henblik på anvendelsen af denne artikels stk. 1 lagrer eu-LISA de i stk. 1 omhandlede data i det centrale register med henblik på rapportering og statistik som omhandlet i [artikel 39 i forordning 2018/XX om interoperabilitet]."

26) I artikel 63, stk. 4, indsættes et nyt afsnit:

"De daglige statistikker lagres i det centrale register for rapportering og statistik."

Artikel 55c
Ændringer af Rådets beslutning 2004/512/EF

I Rådets beslutning 2004/512/EF om indførelse af visuminformationssystemet (VIS) foretages følgende ændringer:

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

"2. Visuminformationssystemet baseres på en centraliseret arkitektur og skal bestå af:

a) det fælles identitetsregister som omhandlet i [artikel 17, stk. 2, litra a), i forordning 2018/XX om interoperabilitet]

b) et centralt informationssystem, i det følgende benævnt "det centrale visuminformationssystem" (CS-VIS)

c) en grænseflade i hver medlemsstat, i det følgende benævnt "den nationale grænseflade" (NI-VIS), der skal fungere som bindeled til den relevante centrale nationale myndighed i de enkelte medlemsstater

d) kommunikationsinfrastrukturen mellem det centrale visuminformationssystem og de nationale grænseflader

e) en sikker kommunikationskanal mellem ind- og udrejsesystemets centrale system og CS-VIS

f) en sikker kommunikationsinfrastruktur mellem CS-VIS og de centrale infrastrukturer i den europæiske søgeportal oprettet ved [artikel 6 i forordning 2018/XX om interoperabilitet], den fælles biometriske matchtjeneste oprettet ved [artikel 12 i forordning 2018/XX om interoperabilitet], det fælles identitetsregister og multiidentitetsdetektoren (MID) oprettet ved [artikel 25 i forordning 2018/XX om interoperabilitet]".

Artikel 55d
Ændringer af forordning (EF) nr. 767/2008

1) I artikel 1 indsættes følgende stykke:

"2. "Ved at lagre identitetsdata, rejsedokumenter og biometriske data i det fælles identitetsregister oprettet ved [artikel 17 i forordning 2018/XX om interoperabilitet] bidrager VIS til at lette og bistå med en korrekt identifikation af personer registreret i VIS på de betingelser og med henblik på det endelige mål, der er fastsat i stk. 1 i denne artikel."

2) I artikel 4 tilføjes følgende numre:

"12) "VIS-data": alle data lagret i det centrale VIS-system og i det fælles identitetsregister, jf. artikel 9-14

"13) "identitetsdata": de data, der er omhandlet i artikel 9, stk. 4, litra a)-aa)

14) "fingeraftryksdata": data om de fem fingeraftryk af pegefingeren, langfingeren, ringfingeren, lillefingeren og tommelfingeren på højre hånd, hvis de findes, og på venstre hånd

15) "ansigtsbillede": digitale billeder af ansigtet

16) "biometriske data": fingeraftryksdata og ansigtsbillede"

3) I artikel 5 indsættes følgende stykke:

"1a). Det fælles identitetsregister indeholder de data, der er omhandlet i artikel 9, stk. 4, litra a)-cc), artikel 9, stk. 5, og artikel 9, stk. 6, mens de resterende VIS-data lagres i det centrale VIS-system."

4) I artikel 6, stk. 2, foretages følgende ændringer:

"2. Adgangen til VIS med henblik på at søge oplysninger er udelukkende forbeholdt behørigt bemyndigede medarbejdere i de nationale myndigheder i hver medlemsstat, som er kompetente med hensyn til de formål, der er fastsat i artikel 15-22, og behørigt bemyndigede medarbejdere i de nationale myndigheder i hver enkelt medlemsstat og

EU's organer, som er kompetente med hensyn til de formål, der er fastsat i [artikel 20 og artikel 21 i forordning 2018/XX om interoperabilitet], og er begrænset til de oplysninger, der er nødvendige for udførelsen af deres opgaver i overensstemmelse med disse formål og står i rimeligt forhold til de forfulgte mål."

5) Artikel 9, stk. 4, litra a) til c), ændres således:

"a) efternavn, (familienavn), fornavn(e), (døbenavn(e)), fødselsdato, nationalitet(er), køn

aa) fødenavn (tidligere efternavn(e)), fødeby og -land, nationalitet ved fødslen

b) rejsedokumentets eller -dokumenternes type og nummer og koden bestående af tre bogstaver for det land, der har udstedt rejsedokumentet eller -dokumenterne

c) datoen for rejsedokumentets eller -dokumenternes udløb

cc) den myndighed, der har udstedt rejsedokumentet, og datoen for dets udstedelse

6) Artikel 9, stk. 5, affattes således:

"ansigtsbillede som defineret i artikel 4, stk. 15".

7) I artikel 29, stk. 2, litra a), erstattes "VIS" af "VIS eller det fælles identitetsregister" i de to tilfælde, hvor det forekommer.

Artikel 55e
Ændringer af Rådets afgørelse 2008/633/RIA

1) I artikel 5 indsættes som stk. 1a:

"1a. I tilfælde, hvor de udpegede myndigheder har foretaget en forespørgsel i det fælles identitetsregister, jf. [artikel 22 i forordning 2018/XX om interoperabilitet], kan de få adgang til at konsultere VIS, hvis det modtagne svar som omhandlet i [artikel 22,] stk. 3[, i forordning 2018/XX om interoperabilitet] viser, at der er lagret data i VIS."

2) I artikel 7 indsættes som stk. 1a:

"1a. I tilfælde, hvor Europol har foretaget en forespørgsel i det fælles identitetsregister, jf. [artikel 22 i forordning 2018/XX om interoperabilitet], kan Europol få adgang til VIS med henblik på konsultation, hvis det modtagne svar som omhandlet i [artikel 22,] stk. 3[, forordning 2018/XX om interoperabilitet] viser, at der er lagret data i VIS."

KAPITEL X
Afsluttende bestemmelser

Artikel 56
Rapportering og statistik

1. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og eu-LISA har adgang til at konsultere følgende data vedrørende den europæiske søgeportal (ESP), udelukkende med henblik på rapportering og statistik uden at få mulighed for at identificere enkeltpersoner:

a) antal forespørgsler pr. bruger af ESP-profilen

b) antal forespørgsler til hver af Interpol-databaserne.

2. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og eu-LISA har adgang til at konsultere følgende data

vedrørende det fælles identitetsregister, udelukkende med henblik på rapportering og statistik uden at få mulighed for at identificere enkeltpersoner:

a) antal forespørgsler i medfør af 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 data.

3. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og eu-LISA har adgang til at konsultere følgende data vedrørende multiidentitetsdetektoren, udelukkende med henblik på rapportering og statistik uden at få mulighed for at identificere enkeltpersoner:

a) personens nationalitet, køn og fødselsår

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

c) antal søgninger foretaget med og uden biometriske data

d) antallet af hver type link.

4. De behørigt bemyndigede medarbejdere hos Det Europæiske Agentur for Grænse- og Kystbevogtning oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2016/1624[76] har adgang til at konsultere de data, der er omhandlet i stk. 1, 2 og 3, med henblik på at foretage risikoanalyser og sårbarhedsvurderinger som omhandlet i artikel 11 og 13 i nævnte forordning.

5. Med henblik på anvendelsen af denne artikels stk. 1 lagrer eu-LISA de data, der er omhandlet i denne artikels stk. 1, i det centrale register med henblik på rapportering og statistik som omhandlet i denne forordnings kapitel VII. Dataene i registret giver ikke mulighed for identifikation af enkeltpersoner, men gør det muligt for de myndigheder, der er nævnt i denne artikels stk. 1, at indhente brugertilpassede 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.

Artikel 57
Overgangsperiode for brug af den europæiske søgeportal

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.

Artikel 58
Overgangsperiode for bestemmelserne om adgang til det fælles identitetsregister med henblik på retshåndhævelse

Artikel 22, artikel 55b, nr. 13, 14, 15 og 16, og artikel 55e finder anvendelse fra datoen for idriftsættelsen som omhandlet i artikel 62, stk. 1.

[76] 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 59
Overgangsperiode for multiidentitetsdetektoren

1. I en periode på et år, efter at eu-LISA har underrettet om afslutningen af den test, der henvises til i artikel 62, stk. 1, litra b), om multiidentitetsdetektoren (MID), og før idriftsættelsen af MID, er den centrale ETIAS-enhed, der er omhandlet i [artikel 33, litra a), i forordning (EU) 2016/1624] ansvarlig for at påvise flere identiteter blandt de data, der er lagret i VIS, Eurodac og SIS. Påvisning af flere identiteter foretages udelukkende ved hjælp af biometriske data, jf. denne forordnings artikel 27, stk. 2.

2. Hvis forespørgslen resulterer i et eller flere hit(s), og identitetsdataene i de sammenkædede filer er identiske eller ensartede, oprettes et hvidt link, jf. artikel 33.

   Hvis forespørgslen resulterer i et eller flere hit(s), og identitetsdataene i de sammenkædede filer ikke kan anses for at være ensartede, oprettes et gult link, jf. artikel 30, og proceduren i artikel 29 finder anvendelse.

   Hvis der rapporteres om adskillige hits, oprettes et link til alle de data, der udløser et hit.

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

4. Hvis der oprettes et link til en indberetning i SIS, bortset fra en indberetning om nægtelse af indrejse eller en indberetning om et rejsedokument, der er meldt bortkommet, stjålet eller ugyldiggjort, jf. artikel 24 i SIS-forordningen inden for grænsekontrol og artikel 38 i SIS-forordningen inden for retshåndhævelse, giver MID SIRENE-kontoret i den medlemsstat, der oprettede indberetningen, adgang til de identitetsdata, der findes i de forskellige informationssystemer.

5. Den centrale ETIAS-enhed eller SIRENE-kontoret i den medlemsstat, der oprettede indberetningen, har adgang til de data, der findes i identitetsbekræftelsesfilen, og vurderer de forskellige identiteter og ajourfører linket i henhold til artikel 31, 32 og 33 og føjer det til identitetsbekræftelsesfilen.

6. eu-LISA bistår om nødvendigt den centrale ETIAS-enhed med at påvise flere identiteter som omhandlet i denne artikel.

Artikel 60
Omkostninger

1. Omkostningerne til etablering og drift af ESP, den fælles biometriske matchtjeneste, det fælles identitetsregister og MID afholdes over EU's 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 EU's 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. De udpegede myndigheders omkostninger, der er omhandlet i artikel 4, stk. 24, afholdes af henholdsvis den enkelte medlemsstat og Europol. Omkostningerne til at forbinde de udpegede myndigheder med det fælles identitetsregister afholdes af henholdsvis den enkelte medlemsstat og Europol.

Artikel 61
Meddelelser

1. Medlemsstaterne meddeler eu-LISA de myndigheder, der er omhandlet i stk. 7, 20, 21 og 26, som kan benytte eller få adgang til henholdsvis ESP, det fælles identitetsregister 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, jf. artikel 62. Hvis der sker ændringer heri, offentliggør eu-LISA en ajourført konsolideret liste en gang om året.

2. eu-LISA underretter Kommissionen, når den test, der er omhandlet i artikel 62, stk. 1, litra b), er afsluttet på tilfredsstillende vis.

3. Den centrale ETIAS-enhed underretter Kommissionen, når overgangsforanstaltningen, der er fastsat i artikel 59, er afsluttet på vellykket vis.

4. Kommissionen stiller de meddelte oplysninger, jf. stk. 1, til rådighed for medlemsstaterne og offentligheden via et konstant opdateret offentligt websted.

Artikel 62
Idriftsættelse

1. Kommissionen beslutter, fra hvilken dato hver interoperabilitetskomponent skal idriftsættes, efter at følgende betingelser er opfyldt:

   a) De foranstaltninger, der er omhandlet i artikel 8, stk. 2, artikel 9, stk. 7, artikel 28, stk. 5 og 6, artikel 37, stk. 4, artikel 38, stk. 4, artikel 39, stk. 5, og artikel 44, stk. 5 er blevet vedtaget.

   b) eu-LISA har erklæret, at en omfattende test af den relevante interoperabilitetskomponent, som skal udføres af eu-LISA i samarbejde med medlemsstaterne, er gennemført på vellykket vis.

   c) eu-LISA har valideret de tekniske og juridiske foranstaltninger for at indsamle og fremsende de i artikel 8, stk. 1, og artikel 13, 19, 34 og 39 omhandlede data og har underrettet Kommissionen derom.

   d) Medlemsstaterne har underrettet Kommissionen som omhandlet i artikel 61, stk. 1.

   e) For så vidt angår multiidentitetsdetektoren har den centrale ETIAS-enhed underrettet Kommissionen som omhandlet i artikel 61, stk. 3.

2. Kommissionen meddeler Europa-Parlamentet og Rådet resultaterne af den test, som er udført i henhold til stk. 1, litra b).

3. Kommissionens afgørelse, jf. stk. 1 offentliggøres i *Den Europæiske Unions Tidende*.

4. Medlemsstaterne og Europol begynder at bruge interoperabilitetskomponenterne fra den dato, der fastsættes af Kommissionen efter stk. 1.

Artikel 63
Udøvelse af de delegerede beføjelser

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

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 8, stk. 2, og artikel 9, stk. 7, tillægges Kommissionen for en ubestemt periode fra [*datoen for denne forordnings ikrafttræden*].

3. Den i artikel 8, stk. 2, og artikel 9, stk. 7, omhandlede uddelegering 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 samtidig Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 8, stk. 2, og artikel 9, stk. 7, 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 informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med [to måneder] på Europa-Parlamentets eller Rådets initiativ.

Artikel 64
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.

Artikel 65
Rådgivende gruppe

eu-LISA nedsætter en rådgivende gruppe for at få ekspertise vedrørende interoperabilitet, navnlig inden for rammerne af udarbejdelsen af det årlige arbejdsprogram og den årlige aktivitetsrapport. Under projekterings- og udviklingsfasen af interoperabilitetsinstrumenterne gælder artikel 52, stk. 4-6.

Artikel 66
Uddannelse

eu-LISA udfører opgaver vedrørende uddannelse i den tekniske anvendelse af interoperabilitetskomponenterne i overensstemmelse med forordning (EU) nr. 1077/2011.

Artikel 67
Praktisk vejledning

Kommissionen udarbejder i tæt samarbejde med medlemsstaterne, eu-LISA og andre relevante 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 68
Overvågning og evaluering

1. eu-LISA sikrer, at der er indført procedurer med henblik på at følge udviklingen af interoperabilitetskomponenterne 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 [*seks måneder efter denne forordnings ikrafttræden* – OPOCE, please replace with the actual date] og derefter hver sjette måned under udviklingsfasen for interoperabilitetskomponenterne forelægger eu-LISA en rapport for Europa-Parlamentet og Rådet om status over udviklingen af interoperabilitetskomponenterne. Når systemet er færdigudviklet, 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. Med henblik på den tekniske vedligeholdelse har eu-LISA adgang til de nødvendige oplysninger vedrørende databehandlingsprocesserne i interoperabilitetskomponenterne.

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

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

   a) en vurdering af denne forordnings anvendelse

   b) en gennemgang af de opnåede resultater set i forhold til målene og indvirkningen på de grundlæggende rettigheder

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

   d) en vurdering af sikkerheden ved interoperabilitetskomponenterne

   e) en vurdering af eventuelle konsekvenser, herunder eventuelle uforholdsmæssigt store virkninger for trafikstrømmen ved grænseovergangssteder, og konsekvenser med budgetmæssige virkninger for EU's budget.

Evalueringen skal omfatte eventuelle nødvendige henstillinger. Kommissionen sender evalueringsrapporten til Europa-Parlamentet, Rådet, Den Europæiske Tilsynsførende for Databeskyttelse og Den Europæiske Unions Agentur for Grundlæggende Rettigheder, som er oprettet ved Rådets forordning (EF) nr. 168/2007[77].

6. Medlemsstaterne og Europol sender eu-LISA og Kommissionen de oplysninger, som er nødvendige for at udarbejde de i stk. 4 og 5 nævnte rapporter. Disse oplysninger må ikke påvirke arbejdsmetoder negativt eller omfatte oplysninger, som afslører kilder, medarbejdere eller undersøgelser hos de udpegede myndigheder.

7. eu-LISA sender Kommissionen de oplysninger, der er nødvendige for at foretage de evalueringer, der er omhandlet i stk. 5.

8. Medlemsstaterne og Europol aflægger under overholdelse af national lovgivning om offentliggørelse af følsomme oplysninger hver deres årsrapport om, hvor effektiv adgangen til data lagret i det fælles identitetsregister har været med henblik på retshåndhævelse, idet rapporterne skal indeholde oplysninger og statistisk materiale om:

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

   b) en rimelig begrundelse for den begrundede mistanke om, at den mistænkte, gerningsmanden eller offeret er omfattet af [ind- og udrejsesystemet], VIS-forordningen eller [ETIAS-forordningen]

   c) antallet af anmodninger om adgang til det fælles identitetsregister med henblik på retshåndhævelse

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

   e) behovet for og anvendelsen af reglen om ekstraordinære tilfælde af hastende karakter, herunder de tilfælde, hvor tilfældets hastende karakter ikke blev accepteret ved den efterfølgende kontrol, der foretages af det centrale adgangspunkt.

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

Artikel 69
Ikrafttræden og anvendelse

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

[77] 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).

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

Udfærdiget i Strasbourg, den […].

På Europa-Parlamentets vegne	*For Rådet*
Formanden	*Formanden*

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

1.2. Berørt(e) politikområde(r)

1.3. Forslagets/initiativets art

1.4. Mål

1.5. Forslagets/initiativets begrundelse

1.6. Varighed og finansielle virkninger

1.7. Påtænkt(e) forvaltningsmetode(r)

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om overvågning og rapportering

2.2. Forvaltnings- og kontrolsystem

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftspost(er) på budgettet og udgiftsområde(r) i den flerårige finansielle ramme

3.2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af de anslåede virkninger for udgifterne

3.2.2. Anslåede virkninger for aktionsbevillingerne

3.2.3. Anslåede virkninger for administrationsbevillingerne

3.2.4. Forenelighed med den nuværende flerårige finansielle ramme

3.2.5. Tredjemands bidrag til finansieringen

3.3. Anslåede virkninger for indtægterne

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af interoperabilitet mellem EU's informationssystemer for sikkerhed, grænse- og migrationsforvaltning.

1.2. Berørt(e) politikområde(r)

Indre anliggender (afsnit 18)

1.3. Forslagets/initiativets art

X Forslaget/initiativet vedrører **en ny foranstaltning**

☐ Forslaget/initiativet drejer sig om **en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning**[78]

☐ Forslaget/initiativet vedrører **en forlængelse af en eksisterende foranstaltning**

☐ Forslaget/initiativet vedrører **omlægning af en foranstaltning til en ny foranstaltning**

1.4. Mål

1.4.1. Det eller de af Kommissionens flerårige strategiske mål, som forslaget/initiativet vedrører

Grænseforvaltning – redde liv og sikre de ydre grænser

Interoperabilitetskomponenterne giver mulighed for en bedre udnyttelse af de oplysninger, der er indeholdt i de eksisterende EU-systemer for sikkerhed, grænse- og migrationsforvaltning. Disse foranstaltninger undgår hovedsagelig, at den samme person registreres i forskellige systemer med forskellige identiteter. I øjeblikket er det muligt at foretage en unik identifikation af en person inden for et givent system, men ikke på tværs af systemerne. Dette kan føre til fejlagtige beslutninger fra myndighedernes side eller omvendt bruges af rejsende i ond tro til at skjule deres rigtige identitet.

Bedre informationsudveksling

De foreslåede foranstaltninger giver også de retshåndhævende myndigheder en effektiv, men dog afgrænset adgang til disse data. Men i modsætning til situationen i dag er der ét sæt betingelser snarere end et forskelligt sæt for hver dataindsamling.

1.4.2. Specifik(ke) målsætning(er) og specifikt mål nr. [ ]

Fastlæggelsen af interoperabilitetskomponenterne har følgende generelle mål:

(a) at forbedre forvaltningen af de ydre grænser

(b) at bidrage til forebyggelse og bekæmpelse af irregulær migration og

[78] Jf. finansforordningens artikel 54, stk. 2, litra a) eller b).

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

Målene for at sikre interoperabilitet skal opnås ved at:

a) sikre korrekt identifikation af personer

b) bidrage til bekæmpelse af identitetssvig

c) forbedre og harmonisere datakvalitetskrav i de respektive EU-informationssystemer

d) lette den tekniske og operationelle gennemførelse i medlemsstaterne af eksisterende og fremtidige EU-informationssystemer

e) styrke og forenkle de betingelser for datasikkerhed og databeskyttelse, der styrer de respektive EU-informationssystemer, og gøre dem mere ensartede

f) forenkle og ensrette betingelserne for retshåndhævende myndigheders adgang til ind- og udrejsesystemet, VIS, ETIAS og Eurodac

g) støtte formålet med ind- og udrejsesystemet, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN-systemet

Berørt(e) ABM/ABB-aktivitet(er)

Kapitlet Sikkerhed og beskyttelse af frihedsrettigheder: Intern sikkerhed

1.4.3. Forventede resultater og virkninger

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgruppen.

De generelle målsætninger for dette initiativ stammer fra de to traktatfæstede mål:

1. At forbedre forvaltningen af Schengenområdets ydre grænser på grundlag af den europæiske dagsorden for migration og efterfølgende meddelelser, herunder meddelelsen om bevarelse og styrkelse af Schengenområdet.

2. At bidrage til den indre sikkerhed i Den Europæiske Union på grundlag af den europæiske dagsorden om sikkerhed og Kommissionens arbejde om indførelse af en effektiv og ægte sikkerhedsunion.

De specifikke politiske mål for dette interoperabilitetsinitiativ er:

Dette forslags specifikke mål er:

1. at sikre, at slutbrugerne, navnlig grænsevagter, retshåndhævende myndigheder, immigrationsmyndighederne og retlige myndigheder får hurtig, problemfri, systematisk og kontrolleret adgang til de oplysninger, som de behøver for at varetage deres opgaver

2. at levere en løsning til at påvise flere identiteter knyttet til det samme sæt biometriske data med det dobbelte formål at sikre korrekt identificering af personer i god tro og bekæmpe identitetssvig

3. at lette politimyndighedernes identitetskontrol af tredjelandsstatsborgere på en medlemsstats område og

4. at lette og effektivisere retshåndhævende myndigheders adgang til informationssystemer, som ikke vedrører retshåndhævelse, på EU-niveau, hvor det er nødvendigt for at forebygge, efterforske, opdage eller retsforfølge alvorlige strafbare handlinger og terrorisme.

For at opfylde det specifikke mål nr. 1 udvikles den europæiske søgeportal (ESP).

For at opfylde det specifikke mål nr. 2 indføres multiidentitetsdetektoren (MID) støttet af det fælles identitetsregister og den fælles biometriske matchtjeneste (BMS).

For at opfylde det specifikke mål nr. 3 gives bemyndigede tjenestemænd adgang til det fælles identitetsregister med henblik på identifikation.

For at opfylde mål nr. 4 indeholder det fælles identitetsregister en funktion til hit/intet hit-påtegning, der muliggør en totrinstilgang for retshåndhævende myndigheders adgang til grænseforvaltningssystemer.

Ud over disse fire interoperabilitetskomponenter understøttes målene i afsnit 1.4.2 endvidere af oprettelsen og forvaltningen af det universelle meddelelsesformat (UMF) som en EU-standard til udvikling af informationssystemer på området retlige og indre anliggender og oprettelsen af et fælles register til rapportering og statistik (CRRS).

1.4.4. Virknings- og resultatindikatorer

Angiv indikatorerne til kontrol af forslagets/initiativets gennemførelse.

Hver af de foreslåede foranstaltninger kræver udvikling, efterfulgt af vedligeholdelse og drift, af den pågældende komponent.

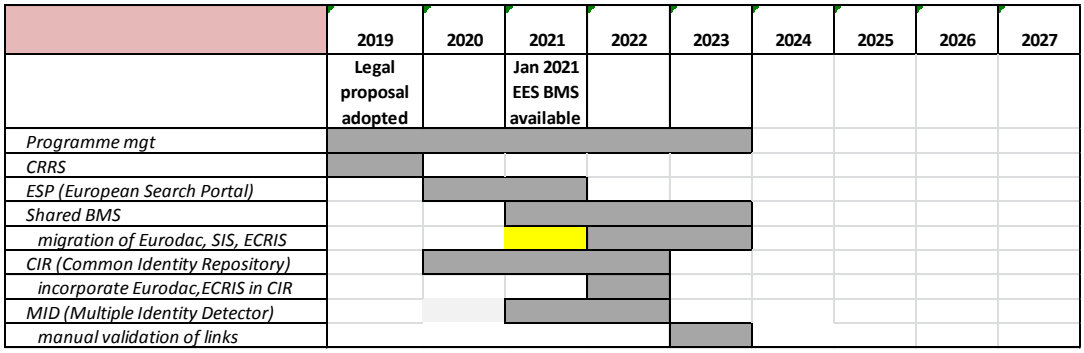
Under udviklingen

Udviklingen af hver komponent sker, når forudsætningerne herfor er opfyldt, dvs. at den foreslåede retsakt er vedtaget af lovgiverne, og de tekniske forudsætninger er opfyldt, da visse komponenter først kan opbygges, når en anden er tilgængelig.

Særlig målsætning: klar til drift pr. måldatoen

Ved udgangen af 2017 sendes forslaget til lovgiverne med henblik på vedtagelse. Det antages, at vedtagelsesproceduren vil blive afsluttet i løbet af 2018, alt efter den tid, det tager for de andre forslag.

Under denne forudsætning fastsættes begyndelsen af udviklingsperioden til begyndelsen af 2019 (= T0) for at få et referencepunkt, hvorfra varighed regnes, og ikke absolutte datoer. Hvis lovgiverne vedtager forslaget på et senere tidspunkt, forskydes hele tidsplanen i overensstemmelse hermed. På den anden side skal den fælles BMS være tilgængelig, før det fælles identitetsregister og MID kan fuldføres. Varigheden af udviklingen fremgår af skemaet nedenfor:



(gul markering viser en specifik opgave vedrørende Eurodac).

- centralt register til rapportering og statistik (CRRS): frist: T0 + 12 måneder (2019-2020)

- europæisk søgeportal (ESP): frist: T0 + 36 måneder (2019-2021)

- den fælles biometriske matchtjeneste (fælles BMS) oprettes først til at levere ind- og udrejsesystemet. Når denne milepæl er nået, skal de applikationer, som bruger den fælles BMS, ajourføres, og dataene i det automatiske fingeraftryksidentifikationssystem i SIS (AFIS), AFIS i Eurodac og dataene i ECRIS-TCN skal overføres til den fælles BMS. Fristen for gennemførelse er udgangen af 2023.

- Det fælles identitetsregister oprettes først under implementeringen af ind- og udrejsesystemet. Når ind- og udrejsesystemet er afsluttet, indlæses dataene fra Eurodac og ECRIS i det fælles identitetsregister. Fristen for afslutning er ultimo 2022 (tilgængelighed af den fælles BMS + 12 måneder).

- Multiidentitetsdetektoren (MID) oprettes efter idriftsættelsen af det fælles identitetsregister. Fristen for afslutning er ultimo 2022 (tilgængelighed af den fælles BMS + 24 måneder), men der er en meget ressourcekrævende periode til validering af links mellem identiteter, der foreslås af MID. Hvert af de estimerede links skal valideres manuelt. Dette finder sted frem til udgangen af 2023.

Driftsperioden begynder, når ovennævnte udviklingsperiode er afsluttet.

Drift

Indikatorerne i tilknytning til de enkelte specifikke mål i 1.4.3 er som følger:

1. Særlig målsætning: Hurtig, problemfri og systematisk adgang til autoriserede datakilder

- Antal gennemførte anvendelser (= antal søgninger, der kan håndteres af ESP) pr. periode.

- Antal søgninger håndteret af ESP sammenlignet med det samlede antal søgninger (via ESP og systemer direkte) pr. periode.

2. Særlig målsætning: Påvise flere identiteter

- Antal identiteter knyttet til det samme sæt biometriske data sammenlignet med antal identiteter med biografiske oplysninger pr. periode.

- Antal afslørede tilfælde af identitetssvig sammenlignet med antal tilknyttede identiteter og det samlede antal identiteter pr. periode.

3. Særlig målsætning: Lette identifikationen af tredjelandsstatsborgere

– Antal identifikationskontroller sammenlignet med det samlede antal transaktioner pr. periode.

4. Særlig målsætning: Forenkle adgangen til autoriserede datakilder med henblik på retshåndhævelse

- Antal adgange i "trin 1" (= kontrol af dataenes tilstedeværelse) til retshåndhævelsesformål pr. periode.

- Antal adgange i "trin 2" (= den faktiske konsultation af data fra EU's systemer inden for anvendelsesområdet) til retshåndhævelsesformål pr. periode.

5. Tværgående, supplerende mål: At forbedre kvaliteten af data og anvendelse af data til bedre politisk beslutningstagning

- Løbende udarbejdelse af rapporter om overvågning af datakvalitet.

- Antal ad hoc-forespørgsler om statistiske oplysninger pr. periode.

1.5. Forslagets/initiativets begrundelse

1.5.1. Krav, der skal opfyldes på kort eller lang sigt

Som påvist i den konsekvensanalyse, der ledsager dette juridiske forslag, er de respektive foreslåede komponenter nødvendige for at opnå interoperabilitet:

- For at opfylde målet om at give autoriserede brugere hurtig, problemfri, systematisk og kontrolleret adgang til relevante informationssystemer bør der oprettes en europæisk søgeportal (ESP), der bygger på en fælles BMS til alle databaser.

- For at opfylde målet om at lette bemyndigede medarbejderes identitetskontrol af tredjelandsstatsborgere på en medlemsstats område bør der oprettes et fælles identitetsregister, som indeholder et minimumssæt af identifikationsdata og bygger på samme fælles BMS.

- For at opfylde målet om at påvise flere identiteter forbundet med samme sæt biometriske data med det dobbelte formål at lette identitetskontrol af rejsende i god tro og bekæmpe identitetssvig bør der oprettes en multiidentitetsdetektor (MID), som indeholder links mellem flere identiteter på tværs af systemerne.

• For at opfylde målet om at lette og effektivisere de retshåndhævende myndigheders adgang til informationssystemer, der ikke vedrører retshåndhævelse, med henblik på at forebygge, efterforske, opdage eller retsforfølge alvorlige strafbare handlinger og terrorisme, bør det fælles identitetsregister indeholde en funktion til hit/intet hit-påtegning.

Da alle målene skal opfyldes, er den fuldstændige løsning en kombination af ESP, det fælles identitetsregister (med hit/intet hit-påtegning) og MID, som alle benytter den fælles BMS.

1.5.2. Merværdien ved en indsats fra EU's side (det kan skyldes forskellige faktorer, f.eks. fordele ved koordination, retssikkerhed, større effektivitet eller komplementaritet). I dette punkt forstås ved "den merværdi, der skabes ved Unionens deltagelse" den værdi, der skyldes Unionens medvirken, og som rækker ud over den værdi, der ellers ville være skabt af medlemsstaterne alene.

Der er brug for foranstaltninger på europæisk plan, fordi de systemer, der foreslås at skulle gøres interoperable, er systemer, der anvendes af flere medlemsstater: enten alle medlemsstater (Eurodac) eller alle medlemsstater, der er en del af Schengenområdet (ind- og udrejsesystemet, VIS, ETIAS og SIS). Foranstaltningerne kan pr. definition ikke blot træffes på et andet plan.

Den vigtigste forventede merværdi er at fjerne tilfælde af identitetssvig, kortlægge de tilfælde, hvor en person har brugt forskellige identiteter til at komme ind i EU, og undgå at personer i god tro bliver forvekslet med personer i ond tro med samme navn. En yderligere merværdi er, at den interoperabilitet, der foreslås her, skaber mulighed for en gennemførelse og vedligeholdelse af EU's store it-systemer. For retshåndhævende myndigheder bør de foreslåede foranstaltninger resultere i en mere hyppig og vellykket adgang til bestemte data inden for EU's store it-systemer. På operationelt plan kan kvaliteten af data kun vedligeholdes og forbedres, hvis de overvåges. Endvidere er der, for så vidt angår politik og beslutningstagning, behov for at gøre det muligt at foretage ad hoc-forespørgsler om anonymiserede data.

En cost-benefit-analyse er en del af konsekvensanalysen og tager kun højde for de fordele, der kan kvantificeres, og de forventede fordele kan derfor med rimelighed estimeres til omkring 77,5 mio. EUR om året og tilfalder primært medlemsstaterne. Disse fordele skyldes i det væsentlige:

- Reducerede omkostninger til ændringer af nationale applikationer, når det centrale system er idriftsat (anslået til 6 mio. EUR pr. år for medlemsstaternes it-afdelinger).

- Omkostningsbesparelser ved at have én central fælles BMS i stedet for én BMS pr. centralt system, der indeholder biometriske data (anslået til 1,5 mio. EUR pr. år og en besparelse på 8 mio. EUR for eu-LISA).

- Sparede omkostninger til identifikation af flere identiteter sammenlignet med den situation, hvor det samme resultat kan opnås uden det foreslåede middel. Dette ville betyde en omkostningsbesparelse på mindst 50 mio. EUR pr. år for medlemsstaternes administrationer for grænseforvaltning, migration og retshåndhævelse.

- Omkostningsbesparelse til uddannelse af en stor gruppe slutbrugere sammenlignet med en situation, hvor regelmæssig uddannelse er nødvendig, anslået

til 20 mio. EUR om året til medlemsstaternes administrationer for grænseforvaltning, migration og retshåndhævelse.

1.5.3. Erfaringer fra lignende foranstaltninger

Erfaring fra udviklingen af anden generation af Schengen (SIS II) og af visuminformationssystemet (VIS) viste følgende:

1. For i så høj grad som muligt at undgå budgetoverskridelser og forsinkelser, der skyldes ændrede krav, vil nye informationssystemer inden for området med frihed, sikkerhed og retfærdighed, navnlig hvis der er tale om et stort it-system, ikke blive udviklet, før de grundlæggende retlige instrumenter, der fastsætter formål, anvendelsesområde, funktioner og tekniske detaljer, er endeligt vedtaget.

2. For SIS II's og VIS' vedkommende kunne medlemsstaternes nationale udviklingsarbejde samfinansieres inden for rammerne af Fonden for De Ydre Grænser (EBF), men dette var ikke obligatorisk. Det var derfor ikke muligt at få et overblik over udviklingsniveauet i de medlemsstater, der ikke havde forudset de respektive foranstaltninger i deres flerårige programmering eller manglede præcision i deres programmering. Derfor foreslås det nu, at Kommissionen refunderer alle integrationsomkostninger afholdt af medlemsstaterne for at kunne følge med status for denne udvikling.

3. For at lette den generelle koordinering af gennemførelsen vil alle de foreslåede udvekslinger af meddelelser mellem nationale og centrale systemer genbruge de eksisterende netværk og den nationale ensartede grænseflade.

1.5.4. Sammenhæng med andre relevante instrumenter og eventuel synergivirkning

Kompatibilitet med den nuværende flerårige finansielle ramme

Forordningen om Fonden for Intern Sikkerhed (ISF) er det finansielle instrument, hvor budgettet for gennemførelsen af interoperabilitetsinitiativet indgår.

Den bestemmer i artikel 5, litra b), at 791 mio. EUR skal anvendes til gennemførelsen af et program til udvikling af it-systemer baseret på eksisterende og/eller nye it-systemer til forvaltning af migrationsstrømme på tværs af Unionens ydre grænser, med forbehold af vedtagelsen af de relevante lovgivningsmæssige EU-retsakter og på de betingelser, der er fastsat i artikel 15, stk. 5. Af disse 791 mio. EUR er 480,2 mio. EUR afsat til udvikling af ind- og udrejsesystemet, 210 mio. EUR til ETIAS og 67,9 mio. EUR til revision af SIS II. Den resterende del (32,9 mio. EUR) omfordeles ved hjælp af ISF-B-mekanismer. Det nuværende forslag kræver 32,1 mio. EUR for den nuværende flerårige finansielle rammeperiode, hvilket passer med det resterende budget.

Det nuværende forslag kræver et budget på i alt 424,7 mio. EUR (inklusive udgiftsområde 5) i perioden fra 2019 til 2027. Den nuværende flerårige finansielle ramme dækker kun den toårige periode for 2019 og 2020. Omkostningerne har dog været anslået til og med 2027 for at give et informeret billede af de økonomiske konsekvenser af forslaget og for ikke at foregribe den næste flerårige finansielle ramme.

Det anmodede budget over ni år beløber sig til 424,7 mio. EUR, idet følgende produkter også er omfattet:

1) 136,3 mio. EUR til medlemsstaterne til dækning af ændringerne i deres nationale systemer, så de kan bruge interoperabilitetskomponenterne, den nationale

ensartede grænseflade leveret af eu-LISA og et budget til uddannelse af det væsentlige slutbrugermiljø. Der er ingen indvirkning på den nuværende flerårige finansielle ramme fra 2021 og fremefter.

(2) 4,8 mio. EUR til Det Europæiske Agentur for Grænse- og Kystbevogtning, som er vært for et team af specialister, som i løbet af et år (2023) vil validere sammenhængen mellem identiteter på det tidspunkt, hvor multiidentitetsdetektoren sættes i drift. Teamets aktiviteter kan knyttes sammen med den fjernelse af flertydige identiteter, som tillægges Det Europæiske Agentur for Grænse- og Kystbevogtning i ETIAS-forslaget. Der er ingen indvirkning på den nuværende flerårige finansielle ramme fra 2021 og fremefter.

(3) 48,9 mio. EUR til Europol til at dække opgraderingen af Europols it-systemer til den mængde meddelelser, der skal håndteres, og til det større resultatniveau. Interoperabilitetskomponenterne vil blive anvendt af ETIAS til at udnytte Europols oplysninger. Europols nuværende kapacitet til håndtering af oplysninger er imidlertid ikke i overensstemmelse med de betydelige mængder (i gennemsnit 100 000 standardforespørgsler pr. dag) og den kortere svartid. 9,1 mio. EUR anvendes til den nuværende FFR.

(4) 2,0 mio. EUR til Cepol til dækning af forberedelse og gennemførelse af uddannelse af driftsmedarbejderne. 0,1 mio. EUR er planlagt i 2020.

(5) 225,0 mio. EUR til eu-LISA, hvilket dækker de samlede omkostninger til udvikling af programmet, der leverer de fem interoperabilitetskomponenter (68,3 mio. EUR), omkostningerne til vedligeholdelse af komponenter fra det øjeblik, de leveres, og frem til 2027 (56,1 mio. EUR), et særligt budget på 25,0 mio. EUR til migration af data fra de eksisterende systemer til den fælles BMS og yderligere omkostninger til opdatering af den nationale ensartede grænseflade, netværk, uddannelse og møder. Et specifikt budget på 18,7 mio. EUR dækker omkostningerne ved opgradering og drift af ECRIS-TCN ved høj tilgængelighed fra 2022. Ud af det samlede beløb bruges 23,0 mio. EUR under den nuværende FFR.

(6) 7,7 mio. EUR til GD HOME til dækning af en begrænset forøgelse af personalet og dermed forbundne omkostninger under udviklingsperioden for de forskellige komponenter, eftersom Kommissionen også påtager sig ansvaret for det udvalg, der arbejder med UMF (det universelle meddelelsesformat). Dette budget, der henhører under udgiftsområde 5, er ikke omfattet af ISF-budgettet. Til orientering skyldes der 2,0 mio. EUR i perioden 2019-2020.

Forenelighed med tidligere initiativer

Dette initiativ er foreneligt med følgende:

I april 2016 fremlagde Kommissionen en **Meddelelse om *Stærkere og mere intelligente informationssystemer for grænser og sikkerhed*** for at rette op på en række strukturelle mangler i forbindelse med informationssystemer. Herudfra opstod der tre foranstaltninger:

Først tog Kommissionen **skridt til at styrke og optimere fordelene ved de eksisterende informationssystemer**. I december 2016 vedtog Kommissionen forslag til yderligere styrkelse af det nuværende Schengeninformationssystem (SIS). I mellemtiden, efter Kommissionens forslag i maj 2016, blev forhandlingerne om det reviderede retsgrundlag for Eurodac – EU's asylfingeraftryksdatabase – fremskyndet. Et forslag til et nyt retsgrundlag for visuminformationssystemet (VIS) er også under udarbejdelse og vil blive forelagt i andet kvartal af 2018.

For det andet foreslog Kommissionen **yderligere informationssystemer for at afhjælpe identificerede huller** i EU's datastyringsstruktur. Forhandlingerne om Kommissionens forslag fra april 2016 om oprettelse af et ind- og udrejsesystem[79] – for at forbedre grænsekontrollen for ikke-EU-borgere, der rejser ind i EU – blev afsluttet allerede i juli 2017, da lovgiverne nåede frem til en politisk aftale, som blev bekræftet af Europa-Parlamentet i oktober 2017 og formelt vedtaget af Rådet i november 2017. I november 2016 fremlagde Kommissionen endvidere et forslag om oprettelse af et europæisk system for rejseoplysninger og rejsetilladelser (ETIAS)[80]. Dette forslag sigter mod at styrke sikkerhedskontrollen af visumfri rejsende ved at gøre det muligt på forhånd at foretage kontrol af irregulær migration og sikkerhedskontrol. Lovgiverne forhandler i øjeblikket om dette. I juni 2017 blev det europæiske informationssystem vedrørende strafferegistre for tredjelandsstatsborgere (ECRIS-TCN-systemet)[81] også foreslået for at afhjælpe manglen med hensyn til udveksling af oplysninger mellem medlemsstaterne om dømte tredjelandsstatsborgere.

For det tredje har Kommissionen arbejdet for at skabe **interoperabilitet mellem informationssystemer** med fokus på de fire muligheder, som blev præsenteret i meddelelsen fra april 2016[82] med henblik på at opnå interoperabilitet. Tre af de fire muligheder er netop ESP, det fælles identitetsregister og den fælles BMS. Det stod derefter klart, at der skulle sondres mellem det fælles identitetsregister som database over identiteter og en ny komponent, der identificerer flere identiteter knyttet til samme biometriske identifikator (MID). Så de fire komponenter er nu: ESP, det fælles identitetsregister, MID og den fælles BMS.

Synergi

Synergi forstås her som den fordel, der realiseres ved at genbruge eksisterende løsninger og undgå nye investeringer hele vejen rundt.

Der er også stor synergi mellem disse initiativer og udviklingen af ind- og udrejsesystemet og ETIAS.

Til driften af ind- og udrejsesystemet oprettes en individuel fil for alle tredjelandsstatsborgere, der rejser ind i Schengenområdet på et kortvarigt ophold. Til dette formål udvides den nuværende biometriske matchtjeneste, der anvendes til VIS, og som indeholder fingeraftrykskabeloner til alle visumpåkrævede rejer, til også at omfatte biometriske data fra visumfritagne rejser. Den fælles BMS er således begrebsmæssigt endnu en generalisering af biometrimatchtjenesten, der vil blive opbygget som en del af ind- og udrejsesystemet. De biometriske skabeloner i den biometriske matchtjeneste i SIS og Eurodac overføres derefter (dette er den tekniske betegnelse, når data flyttes fra det ene system til det andet) til den fælles BMS. Ifølge leverandørens data koster lagring i særskilte databaser i gennemsnit 1 EUR pr. biometrisk sæt (der er potentielt 200 mio. datasæt i alt), mens den gennemsnitlige omkostning falder til 0,35 EUR pr. biometrisk sæt, når der oprettes en fælles BMS-løsning. De højere omkostninger til den hardware, der kræves til en stor mængde data, opvejer delvist disse fordele, men i sidste ende skønnes omkostningerne til en fælles BMS at være 30 % lavere, end når de samme data lagres i flere mindre BMS-systemer.

[79] KOM(2016) 194 af 6. april 2016.
[80] KOM(2016) 731 af 16. november 2016.
[81] KOM(2017) 344 af 29. juni 2017.
[82] KOM(2016) 205 af 6. april 2016.

For at ETIAS kan fungere, skal der findes en komponent til forespørgsler i en række EU-systemer. Enten anvendes ESP, eller der opbygges en specifik komponent som en del af forslaget om ESP. Forslaget om interoperabilitet gør det muligt at opbygge én komponent i stedet for to.

Der opnås også synergi ved at genbruge den samme nationale ensartede grænseflade, som bruges til ind- og udrejsesystemet og ETIAS. Den nationale ensartede grænseflade skal opdateres, men vil fortsat blive anvendt.

1.6. Varighed og finansielle virkninger

☐ Forslag/initiativ af **begrænset varighed**

– ☐ Forslag/initiativ gældende fra [DD/MM]ÅÅÅÅ til [DD/MM]ÅÅÅÅ

– ☐ Finansielle virkninger fra ÅÅÅÅ til ÅÅÅÅ

☒ Forslag/initiativ af **ubegrænset varighed**

– Udviklingsperioden fra 2019 til 2023 er inkluderet efterfulgt af fuld drift.

– Varigheden af de finansielle virkninger er derfor fastsat 2019 til 2027.

1.7. Påtænkt(e) forvaltningsmetode(r)[83]

☒ **Direkte forvaltning** ved Kommissionen

– X i dens tjenestegrene inklusive dens personale i EU's delegationer

– ☐ i gennemførelsesorganer

☒ **Delt forvaltning** i samarbejde med medlemsstaterne

☒ **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

– ☐ tredjelande eller organer, som tredjelande har udpeget

– ☐ internationale organisationer og deres organer (angives nærmere)

– ☐Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

– ☒ de organer, der er omhandlet i finansforordningens artikel 208 og 209

– ☐ offentligretlige organer

– ☐ privatretlige organer, der har fået overdraget samfundsopgaver, forudsat at de stiller tilstrækkelige finansielle garantier

– ☐ privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som stiller tilstrækkelige finansielle garantier

– ☐ personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er udpeget i den relevante basisretsakt.

– *Hvis der angives flere forvaltningsmetoder, gives der en nærmere forklaring i afsnittet "Bemærkninger".*

Bemærkninger

Blokke	Udviklingsfase	Driftsfase	Forvaltnings metode	Aktør
Udvikling og vedligeholdelse (af interoperabilitetskomponenter til centrale systemer, uddannelse i system)	X	X	Indirekte	eu-LISA Europol Cepol

[83] Nærmere oplysninger vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Blokke	Udviklingsfase	Driftsfase	Forvaltnings metode	Aktør
Datamigration (overflytning af biometriske skabeloner til en fælles BMS), netværksomkostninger, opdatering af den nationale ensartede grænseflade, møder og uddannelse	X	X	Indirekte	eu-LISA
Validering af links ved oprettelse af MID	X	-	Indirekte	Det Europæiske Agentur for Grænse- og Kystbevogtning
Tilpasning af den nationale ensartede grænseflade, integration af nationale systemer og uddannelse af slutbrugere	X	X	Fælles (eller direkte) (1)	KOM + medlemsstater

1) Der er ingen beløb for driftsfasen inkluderet i dette instrument.

Udviklingsperioden starter fra 2019 og varer indtil leveringen af hver komponent og løber fra 2019 til 2023 (se 1.4.4).

1. Direkte forvaltning i GD HOME: I udviklingsperioden kan foranstaltningerne om nødvendigt gennemføres direkte af Kommissionen. Dette kunne navnlig omfatte Unionens finansielle støtte til aktiviteter i form af tilskud (herunder tilskud til medlemsstaternes nationale myndigheder), offentlige indkøb og/eller godtgørelse af eksterne eksperters udgifter.

2. Delt forvaltning: I udviklingsfasen skal medlemsstaterne tilpasse deres nationale systemer for at få adgang til ESP i stedet for individuelle systemer (dette gælder udgående meddelelser fra medlemsstaterne) og for ændringer i svarene på deres søgeforespørgsler (indgående meddelelser til medlemsstaterne). Der vil ligeledes blive foretaget en opdatering af den eksisterende nationale ensartede grænseflade for ind- og udrejsesystemet og ETIAS.

3. Indirekte forvaltning: eu-LISA vil dække udviklingsdelen af alle projektets it-dele, dvs. interoperabilitetskomponenterne, opdatering af den nationale ensartede grænseflade i hver medlemsstat, opdatering af kommunikationsinfrastrukturen mellem de centrale systemer og de nationale ensartede grænseflader, migration af biometriske skabeloner fra de eksisterende biometriske matchsystemer i SIS og Eurodac til den fælles BMS og den tilhørende datarensningsaktivitet.

I driftsperioden vil eu-LISA udføre alle tekniske aktiviteter i forbindelse med vedligeholdelse af komponenter.

Det Europæiske Agentur for Grænse- og Kystbevogtning vil indføre et ekstra team til validering af links, når MID sættes i drift. Denne opgave har en begrænset varighed.

Europol vil dække udvikling og vedligeholdelse af sine systemer for at sikre interoperabilitet med ESP og ETIAS. Cepol forbereder og gennemfører uddannelse af driftstjenesterne efter princippet om at uddanne underviserne.

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om kontrol og rapportering

Angiv hyppighed og betingelser.

Regler om overvågning og rapportering af udvikling og vedligeholdelse af andre systemer:

1. eu-LISA sikrer, at der er indført procedurer til overvågning af udviklingen af interoperabilitetskomponenterne i lyset af målsætningerne vedrørende planlægning og omkostninger og til overvågning af komponenternes funktion i lyset af målsætninger vedrørende det tekniske output, omkostningseffektivitet, sikkerhed og servicekvalitet.

2. Senest seks måneder efter denne forordnings ikrafttræden og derefter hver sjette måned i udviklingsfasen forelægger eu-LISA en rapport for Europa-Parlamentet og Rådet, hvori der gøres status over udviklingen af de enkelte komponenter. Når systemet er færdigudviklet, indsendes der en rapport til Europa-Parlamentet og Rådet, som i detaljer forklarer, hvordan målene, navnlig vedrørende planlægning og omkostninger, blev opfyldt, samt angiver grundene til eventuelle afvigelser.

3. Med henblik på den tekniske vedligeholdelse har eu-LISA adgang til de nødvendige oplysninger vedrørende databehandlingsprocesserne i komponenterne.

4. Fire år efter idriftsættelsen af den sidste komponent og derefter hvert fjerde år forelægger eu-LISA Europa-Parlamentet, Rådet og Kommissionen en rapport om, hvordan komponenterne fungerer teknisk set.

5. Fem år efter idriftsættelsen af den sidste komponent og derefter hvert fjerde år foretager Kommissionen en samlet evaluering og fremkommer med alle nødvendige henstillinger. Denne samlede evaluering skal omfatte: komponenternes resultater under hensyntagen til målet om interoperabilitet, vedligeholdelsesevne, ydeevne og finansielle følger og indvirkningen på grundlæggende rettigheder.

Kommissionen sender evalueringsrapporten til Europa-Parlamentet og Rådet.

6. Medlemsstaterne og Europol giver eu-LISA og Kommissionen de oplysninger, der er nødvendige for at udarbejde de i stk. 4 og 5 omhandlede rapporter i henhold til de kvantitative indikatorer, som Kommissionen og/eller eu-LISA har fastsat på forhånd. Disse oplysninger må aldrig bringe arbejdsmetoderne i fare eller omfatte oplysninger, som afslører kilder, medarbejderes identitet eller efterforskninger hos de udpegede myndigheder.

7. eu-LISA sender Kommissionen de oplysninger, der er nødvendige for at foretage den samlede evaluering, der er omhandlet i stk. 5.

8. Under overholdelse af bestemmelser i national ret om offentliggørelse af følsomme oplysninger udarbejder hver medlemsstat og Europol årlige rapporter om nyttevirkningen af adgang til EU-systemer til retshåndhævelsesformål, som skal indeholde oplysninger og statistik om:

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

- en rimelig begrundelse for den begrundede mistanke om, at den mistænkte, gerningsmanden eller offeret er omfattet af denne forordning

- antallet af anmodninger om adgang til komponenter med henblik på retshåndhævelse

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

- behovet for og anvendelsen af reglen om ekstraordinære tilfælde af hastende karakter, herunder de tilfælde, hvor tilfældets 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.

2.2. Forvaltnings- og kontrolsystem

2.2.1. Konstaterede risici

Risiciene er dem, der vedrører en it-udvikling af fem komponenter foretaget af en ekstern kontrahent forvaltet af eu-LISA. De typiske projektrisici er følgende:

1. Risikoen for ikke at gennemføre projektet til tiden.

2. Risikoen for ikke at gennemføre projektet inden for budgettet.

3. Risikoen for ikke at levere det fulde omfang af projektet.

Den første risiko er den vigtigste, eftersom en tidsmæssig overskridelse fører til højere omkostninger, da de fleste omkostninger er forbundet med varighed: personaleomkostninger, licensomkostninger pr. år, mv.

Disse risici kan mindskes ved at anvende projektstyringsteknikker, herunder beredskabsplaner i udviklingsprojekter og tilstrækkelig bemanding til at kunne tage toppen af arbejdsbyrden. Arbejdet anslås normalt ved at antage en ligelig arbejdsbyrde spredt over tid, mens projekterne i realiteten har en ulige arbejdsbyrde, der absorberes af højere ressourcetildelinger.

Der er en række risici forbundet med at anvende en ekstern kontrahent til udviklingsarbejdet:

1. navnlig risikoen for, at kontrahenten ikke afsætter tilstrækkelige ressourcer til projektet, eller at kontrahenten udformer og udvikler et system, der ikke har det højeste niveau

2. risikoen for, at administrative teknikker og metoder til at håndtere store it-projekter ikke respekteres fuldt ud som en metode til at reducere kontrahentens omkostninger

3. og endelig kan risikoen for, at kontrahenten får økonomiske problemer af årsager, der ikke har med projektet at gøre, ikke fuldt ud udelukkes.

Disse risici mindskes ved at tildele kontrakter på grundlag af stærke kvalitetskriterier, kontrollere kontrahenternes referencer og bevare et stærkt forhold til dem. Endelig kan der som en sidste udvej indføres skrappe bods- og ophørsklausuler, som kan anvendes, når det er påkrævet.

2.2.2. Oplysninger om det interne kontrolsystem

eu-LISA er tænkt som et videncenter inden for udvikling og forvaltning af store it-systemer. Det gennemfører de aktiviteter, der er forbundet med udviklingen og driften af de forskellige interoperabilitetskomponenter, herunder vedligeholdelse af den nationale ensartede grænseflade i medlemsstaterne.

I udviklingsfasen vil alle udviklingsaktiviteter blive udført af eu-LISA. Dette vil omfatte udviklingsdelen af alle projektets grene. Omkostningerne i forbindelse med integrationen af systemerne i medlemsstaterne i udviklingsfasen forvaltes af Kommissionen via delt forvaltning eller tilskud.

Under driftsfasen vil eu-LISA være ansvarlig for den tekniske og finansielle forvaltning af de komponenter, der anvendes centralt, navnlig tildeling og forvaltning af kontrakter. Kommissionen vil forvalte midlerne til medlemsstaterne for udgifterne til nationale enheder via ISF/Grænser (nationale programmer).

For at undgå forsinkelser på nationalt plan skal der planlægges en effektiv styring mellem alle interessenter, inden udviklingsfasen indledes. Kommissionen antager, at der skal defineres en interoperabel struktur i starten af projektet, som skal anvendes i ind- og udrejsesystemet og ETIAS, da disse projekter leverer og bruger den fælles BMS, det fælles identitetsregister og den europæiske søgeportal. Et medlem af projektstyringsteamet for interoperabilitetsprojektet bør være en del af projektstyringsstrukturen for ind- og udrejsesystemet og ETIAS.

2.2.3. Anslåede omkostninger og fordele ved kontrollen samt forventet fejlrisiko

Der er ikke foretaget nogen skøn, da kontrol og risikobegrænsning er en naturlig opgave for projektstyringsstrukturen.

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger.

De påtænkte foranstaltninger til bekæmpelse af svig er fastsat i artikel 35 i forordning (EU) 1077/2011, hvori følgende bestemmes:

1. Forordning (EF) nr. 1073/1999 finder anvendelse i forbindelse med bekæmpelsen af svig, korruption og andre retsstridige handlinger.

2. Agenturet tiltræder den interinstitutionelle aftale om de interne undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF), og indfører straks passende bestemmelser, som finder anvendelse på hele agenturets personale.

3. I finansieringsafgørelserne samt enhver aftale eller ethvert instrument til gennemførelse heraf fastsættes det udtrykkeligt, at Revisionsretten og OLAF om nødvendigt kan foretage kontrol på stedet hos modtagerne af midler fra agenturet og de organer, der fordeler dem.

I henhold til denne bestemmelse traf bestyrelsen for Det Europæiske Agentur for den Operationelle Forvaltning af Store It-systemer inden for området med Frihed, Sikkerhed og Retfærdighed den 28. juni 2012 afgørelse om betingelserne og de nærmere vilkår for interne undersøgelser i forbindelse med forebyggelse af svig, korruption og alle ulovlige aktiviteter til skade for EU's interesser.

GD HOME's strategi til forebyggelse og opdagelse af svig finder anvendelse.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

DE ANSLÅEDE VIRKNINGER FOR UDGIFTER OG BEMANDING I 2021 OG DEREFTER I DENNE FINANSIERINGSOVERSIGT ER UDELUKKENDE MEDTAGET AF VEJLEDENDE HENSYN OG FOREGRIBER IKKE DEN NÆSTE FLERÅRIGE FINANSIELLE RAMME

3.1. Berørt(e) udgiftspost(er) på budgettet og udgiftsområde(r) i den flerårige finansielle ramme

- Eksisterende poster på budgettet

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgifternes art	Bidrag			
	Nummer [Udgiftsområde……...……]	OB/IOB[84]	fra EFTA-lande[85]	fra kandidatlande[86]	fra tredjelande	iht. finansforordningens artikel 21, stk. 2, litra b)
3	18.02.01.03 – Intelligente grænser	OB	Nej	Nej	Ja	Nej
3	18.02.03 – Det Europæiske Agentur for Grænse- og Kystbevogtning (Frontex)	OB	Nej	Nej	Ja	Nej
3	18.02.04 – Europol	OB	Nej	Nej	Nej	Nej
3	18.02.05 – Cepol	IOB	Nej	Nej	Nej	Nej
3	18.02.07 – Agenturet for Den Operationelle Forvaltning af Store It-systemer inden for Området Frihed, Sikkerhed og Retfærdighed (eu-LISA)	OB	Nej	Nej	Ja	Nej

[84] OB = opdelte bevillinger/IOB = ikkeopdelte bevillinger.
[85] EFTA-lande: Den Europæiske Frihandelssammenslutning
[86] Kandidatlande og, efter omstændighederne, potentielle kandidatlande på Vestbalkan.

3.2. Anslåede virkninger for udgifterne

[Dette afsnit skal udfyldes ved hjælp af **arket vedrørende administrative budgetoplysninger** (det andet dokument i bilaget til denne finansieringsoversigt) og uploades til DECIDE med henblik på høring af andre tjenestegrene.]

3.2.1. Sammenfatning af de anslåede virkninger for udgifterne

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	3	Sikkerhed og EU-borgerskab

GD Home			År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**År 2028**	**I ALT**
• Aktionsbevillinger													
18.02.01.03 – Intelligente grænser	Forpligtelser	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Udbetalinger	(2.	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Administrationsbevillinger finansieret over bevillingsrammen for det specifikke program[87]													
Budgetpostens nummer		(3)											
Bevillinger i alt til GD Home	Forpligtelser	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Udbetalinger	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Udgifterne dækker omkostninger i forbindelse med:

[87] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller aktioner (tidligere BA-poster), indirekte forskning, direkte forskning.

– Omkostninger til tilpasning af den nationale ensartede grænseflade, hvis udvikling finansieres i henhold til forslaget om ind- og udrejsesystemet, et budgetteret beløb til ændringer i systemerne i medlemsstaterne med henblik på at tage hensyn til ændringer af de centrale systemer og et budgetteret beløb til uddannelse af slutbrugere.

18.0203 – Det Europæiske Agentur for Grænse- og Kystbevogtning			År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
Afsnit 1: Personaleudgifter	Forpligtelser	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Udbetalinger	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Afsnit 2: Infrastruktur og driftsudgifter	Forpligtelser	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Udbetalinger	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Afsnit 3: Driftsudgifter	Forpligtelser	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Udbetalinger	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
Bevillinger I ALT til Europol	(Forpligtelser i alt = betalinger i alt)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– Budgettet for Det Europæiske Agentur for Grænse- og Kystbevogtning dækker udgifter til et team til validering af links genereret af MID (multiidentitetsdetektoren) om oprindelige data (omkring 14 mio. registreringer). Mængden af links, der skal valideres manuelt, skønnes at være på omkring 550,000.
Det team, som oprettes til dette formål, føjes til teamet for Det Europæiske Agentur for Grænse- og Kystbevogtning, som oprettes til ETIAS, fordi det er funktionelt tæt på, og man derved undgår omkostningerne til at etablere et nyt team. Arbejdet forventes at finde sted i 2023. De kontraktansatte rekrutteres derfor op til 3 måneder i forvejen, og deres kontrakt ophæves op til 2 måneder efter afslutningen af migrationsaktiviteten. En anden del af de nødvendige ressourcer antages ikke at blive rekrutteret som kontraktansatte og vil blive ansat som konsulenter. Dette forklarer omkostningerne under afsnit 3 for 2023. De antages at blive ansat en måned i forvejen. Yderligere oplysninger om antallet af ansatte gives senere.

– Afsnit 1 omfatter derfor omkostningerne til 20 interne medarbejdere og bestemmelser om en styrkelse af ledelse og hjælpepersonale.

– Afsnit 2 omfatter ekstraomkostninger til 10 ekstra medarbejdere hos kontrahenten.

– Afsnit 3 omfatter gebyret for 10 ekstra medarbejdere hos kontrahenten. Der er ingen andre typer af omkostninger inkluderet.

18.0204 - Europol			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	I ALT
Afsnit 1: Personaleudgifter	Forpligtelser	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Udbetalinger	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Afsnit 2: Infrastruktur og driftsudgifter	Forpligtelser	(1a)	0	0	0	0	0	0	0	0	0	0
	Udbetalinger	(2a)	0	0	0	0	0	0	0	0	0	0
Afsnit 3: Driftsudgifter	Forpligtelser	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Udbetalinger	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
Bevillinger I ALT til Europol	(Forpligtelser i alt = betalinger i alt)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Europols udgifter vil dække opgraderingen af Europols IKT-systemers kapacitet til at håndtere mængden af beskeder, der skal håndteres, og den krævede øgede ydeevne (svartid).

Afsnit 1 Personaleudgifter dækker omkostningerne i forbindelse med ekstra IKT-medarbejdere, der skal ansættes til at styrke Europols informationssystemer af de grunde, der er beskrevet ovenfor. Yderligere oplysninger om fordelingen af stillinger mellem midlertidigt ansatte og kontraktansatte og deres ekspertise er angivet nedenfor.

Afsnit 3 omfatter omkostninger til hardware og software, som skal bruges til at styrke Europols informationssystemer. I øjeblikket betjener Europols it-systemer et begrænset, udpeget miljø bestående af Europol, Europols forbindelsesofficerer og efterforskere i medlemsstaterne, der bruger disse systemer til analytiske og efterforskningsmæssige formål. Med gennemførelsen af QUEST (den systemgrænseflade, som gør det muligt for ESP at foretage forespørgsler i Europols databaser) på et grundlæggende beskyttelsesniveau (Europols informationssystemer er i øjeblikket akkrediteret til et begrænset og fortroligt EU-niveau) vil Europols informationssystemer stilles til rådighed for et meget større autoriseret retshåndhævelsesmiljø. Ud over disse stigninger vil ESP blive brugt af ETIAS til automatisk at forespørge Europols databaser til behandling af rejsetilladelser. Dette vil øge mængden af forespørgsler i forhold til Europols data fra ca. 107 000 forespørgsler om måneden på nuværende tidspunkt til over 100 000 forespørgsler om dagen, ligesom det vil kræve, at Europols informationssystemer er tilgængelige 24/7 og har meget korte svartider for at opfylde kravene i ETIAS-forordningen. Størstedelen af omkostningerne er begrænset til perioden før interoperabilitetskomponenterne idriftsættes, men der er behov for visse løbende forpligtelser for at sikre høj og kontinuerlig adgang til Europols

informationssystemer. Desuden er der behov for visse udviklingsarbejder for at gennemføre interoperabilitetskomponenterne med Europol som bruger.

18.0205 - Cepol			År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
Afsnit 1: Personaleudgifter	Forpligtelser	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Udbetalinger	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Afsnit 2: Infrastruktur og driftsudgifter	Forpligtelser	(1a)	0	0	0	0	0	0	0	0	0	0
	Udbetalinger	(2a)	0	0	0	0	0	0	0	0	0	0
Afsnit 3: Driftsudgifter	Forpligtelser	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Udbetalinger	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Bevillinger I ALT til Cepol	(Forpligtelser i alt = betalinger i alt)	=1+1a +3a	0	0,144	0,384,	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Centralt koordineret EU-uddannelse forbedrer sammenhængende gennemførelse af kurser på nationalt plan og sikrer dermed korrekt og vellykket implementering og anvendelse af interoperabilitetskomponenterne. Cepol er – som EU's Agentur for Uddannelse inden for Retshåndhævelse – godt rustet til at gennemføre uddannelse på centralt EU-plan. Disse udgifter omfatter forberedelse af "uddannelse af medlemsstaternes undervisere", som er nødvendig for at bruge de centrale systemer, når de er blevet interoperable. Omkostningerne omfatter bl.a. en mindre udvidelse af medarbejderstaben i Cepol, som skal koordinere, styre, organisere og opdatere kurserne, og omkostninger til gennemførelse af en række uddannelsessessioner pr. år og forberedelse af onlinekurset. Nærmere oplysninger om disse omkostninger er forklaret nedenfor. Uddannelsesindsatsen koncentreres i de perioder, der ligger umiddelbart forud for go-live. Der er fortsat behov for en vedvarende indsats efter go-live, da interoperabilitetskomponenterne skal vedligeholdes, og underviserne vil ikke fast være de samme personer baseret på erfaringerne med at gennemføre eksisterende uddannelse i Schengeninformationssystemet.

18.0207 - eu-LISA			År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
Afsnit 1: Personaleudgifter	Forpligtelser	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344

	Udbetalinger	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Afsnit 2: Infrastruktur og driftsudgifter	Forpligtelser	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Udbetalinger	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Afsnit 3: Driftsudgifter	Forpligtelser	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Udbetalinger	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Bevillinger I ALT til eu-LISA	(Forpligtelser i alt = betalinger i alt)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Disse udgifter dækker:

– Udvikling og vedligeholdelse af de fire interoperabilitetskomponenter (den europæiske søgeportal (ESP), den fælles biometriske matchtjeneste (fælles BMS), det fælles identitetsregister og multiidentitetsdetektoren (MID), som indgår i forslaget, plus det centrale register til rapportering og statistik (CRRS). eu-LISA vil fungere som repræsentant for projektejeren og bruge egne medarbejdere til at udarbejde specifikationer, udvælge kontrahenter, lede arbejdet, indsende resultater til en række test og acceptere det udførte arbejde.

– Omkostningerne i forbindelse med datamigrationen i ældre systemer til de nye komponenter. eu-LISA spiller dog ikke nogen direkte rolle i den indledende dataindlæsning i MID (validering af links), da dette er en handling, der vedrører selve dataindholdet. Migrationen af biometriske data i ældre systemer omfatter formatet og typen af data og ikke dataindholdet.

– Omkostningerne til opgradering og drift af ECRIS-TCN til et system med høj tilgængelighed fra 2022. ECRIS-TCN er det centrale system, der indeholder straffeattester for tredjelandsstatsborgere. Planen er, at systemet skal blive tilgængeligt i 2020. Interoperabilitetskomponenterne forventes også få adgang til dette system, som derfor også bliver et system med høj tilgængelighed. Driftsudgifterne omfatter ekstraomkostningerne til at opnå denne høje tilgængelighed. Der er betydelige udviklingsomkostninger i 2021 efterfulgt af løbende vedligeholdelses- og driftsomkostninger. Disse omkostninger er ikke medtaget i finansieringsoversigten for revisionen af forordningen om etableringen af eu-LISA[88] som kun omfatter budgetter fra 2018 til 2020 og derfor ikke overlapper med denne budgetanmodning.

[88] COM 2017/0145 (COD) Forslag til Europa-Parlamentets og Rådets forordning om Det Europæiske Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed og om ændring af forordning (EF) nr. 1987/2006 og Rådets afgørelse 2007/533/RIA og om ophævelse af forordning (EU) nr. 1077/2011.

– Udgiftsmønstret skyldes projektrækkefølgen. Da de forskellige komponenter ikke er uafhængige af hinanden, spænder udviklingsperioden fra 2019 til 2023. Men allerede fra 2020 starter vedligeholdelsen og driften af de første tilgængelige komponenter. Dette forklarer, hvorfor udgifterne starter langsomt og derefter øges for til sidst at aftage til en konstant værdi.

– Udgifterne under afsnit 1 (personaleudgifter) følger projektrækkefølgen: Der er behov for flere medarbejdere til at levere projektet hos kontrahenten (hvis udgifter findes under afsnit 3). Når projektet er leveret, overdrages en del af leveringsteamet til udviklings- og vedligeholdelsesarbejde. Samtidig øges antallet af medarbejdere til driften af de nyligt leverede systemer.

– Udgifterne under afsnit 2 (infrastruktur og driftsudgifter) dækker yderligere midlertidige kontorlokaler til kontrahentens team med ansvar for udvikling, vedligeholdelse og driftsopgaver. Udgiftsmønstret over tid følger således også udviklingen i medarbejderstaben. Omkostningerne til opbevaring af ekstraudstyr er allerede medtaget i eu-LISA's budget. Der er heller ingen ekstraomkostninger til eu-LISA's personale, da dette er inkluderet i standardpersonaleomkostningerne.

– Udgifterne under afsnit 3 (driftsudgifter) omfatter udgifter til kontrahenten til udvikling og vedligeholdelse af systemet og indkøb af specifik hardware og software.
  Kontrahentens omkostninger starter i første omgang med undersøgelser af komponenterne og udvikling, i første omgang af en enkelt komponent (CRRS). I perioden 2020-2022 stiger omkostningerne derefter, i takt med at der udvikles flere komponenter parallelt hermed. Omkostningerne falder ikke, når de har nået toppen, da datamigrationsopgaverne er særligt tunge i denne projektportefølje. Kontrahentens omkostninger falder derefter, i takt med at komponenterne leveres og idriftsættes, hvilket kræver et stabilt ressourcemønster.
  Samtidig med udgifterne under afsnit 3 stiger udgifterne i 2020 kraftigt i forhold til det foregående år på grund af den oprindelige investering i hardware og software, som var nødvendig under udviklingen. Udgifterne under afsnit 3 (driftsudgifter) stiger kraftigt i 2021 og 2022, fordi investeringsomkostningerne til henholdsvis hardware og software til de operationelle it-miljøer (produktion og forproduktion for både den centrale enhed og den centrale alternative enhed) afholdes i året før go-live, og interoperabilitetskomponenterne (det fælles identitetsregister og MID) med høje krav til software og hardware. Efter idriftsættelsen er omkostningerne til hardware og software hovedsageligt vedligeholdelsesomkostninger.

– Flere oplysninger findes nedenfor.

Udgiftsområde i den flerårige finansielle ramme	**5**	"Administrationsudgifter"

i mio. EUR (tre decimaler)

		År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
GD HOME											
• Menneskelige ressourcer Budgetpost nr. 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Andre administrative omkostninger (møder mv.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
I ALT GD HOME	Bevillinger	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Bevillinger I ALT under UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme	(I alt forpligtelser = I alt betalinger)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

i mio. EUR (tre decimaler)

		År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	År 2028	**I ALT**
Bevillinger I ALT under UDGIFTSOMRÅDE 1 til 5 i den flerårige finansielle ramme	Forpligtelser	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Udbetalinger	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Anslåede virkninger for aktionsbevillingerne

3.2.2.1. Anslåede virkninger for Det Europæiske Agentur for Grænse- og Kystbevogtnings bevillinger

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater			År **2019**		År **2020**		År **2021**		År **2022**		År **2023**		År **2024**		År **2025**		År **2026**		År **2027**		**I ALT**	
Det Europæiske Agentur for Grænse- og Kystbevogtning Agentur ⇩	Art[89]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[90] Validering af links																						
Antal medarbejdere ansat som eksperter til at validere links	Kontrahentens omkostninger		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Subtotal for specifikt mål nr. 1			**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

[89] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[90] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

Disse udgifter dækker:

- Ansættelse af tilstrækkelig ekstra arbejdskraft (anslået omkring 10 eksperter) til det eksisterende interne personale (anslået omkring 20 personer), som skal arbejde under Det Europæiske Agentur for Grænse- og Kystbevogtning med at validere links. Der er kun en måneds rekruttering før den planlagte startdato til at nå den krævede bemanding.

- Der er ikke anslået andre kontrahentomkostninger. Den software, der kræves, er en del af omkostningerne til den fælles BMS-licens. Der er ikke nogen specifik hardwarebehandlingskapacitet. Kontrahentens medarbejdere antages at høre under Det Europæiske Agentur for Grænse- og Kystbevogtning. Derfor er der under udgifterne i afsnit 2 tilføjet årlige omkostninger til gennemsnitlig 12 kvadratmeter pr. person.

3.2.2.2. Anslåede virkninger for Europols bevillinger

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater **Europol** ⇩			År **2019**		År **2020**		År **2021**		År **2022**		År **2023**		År **2024**		År **2025**		År **2026**		År **2027**		**I ALT**	
	Art[91]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[92] Udvikling og vedligeholdelse af (Europols) systemer																						
It-miljø	Infrastruktur					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
It-miljø	Metalprodukter					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
It-miljø	Software					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948

[91] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[92] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

Udviklingsarbejder	Kontrahent				0,360		0,360												0,720
Subtotal			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Disse udgifter vil dække behovet for at styrke Europols informationssystemer og infrastruktur for at imødekomme stigningen i forespørgsler. Disse omkostninger omfatter:

- opgradering af sikkerhed og netværksinfrastruktur, hardware (servere, lagring) og software (licenser). Disse opgraderinger skal være afsluttet, før den europæiske søgeportal og ETIAS idriftsættes i 2021, og omkostningerne er fordelt ligeligt mellem 2020 og 2021. Fra 2022 er den årlige vedligeholdelse på 20 % brugt som grundlag til at beregne omkostningerne til vedligeholdelse. Hertil kommer, at den femårige standardcyklus til udskiftning af forældet hardware og infrastruktur er taget i betragtning.
- Kontrahentens omkostninger til udviklingsarbejde i forbindelse med at gennemføre QUEST på et grundlæggende beskyttelsesniveau.

3.2.2.3. Anslåede virkninger for Cepols bevillinger

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater **Cepol** ⇩			År **2019**		År **2020**		År **2021**		År **2022**		År **2023**		År **2024**		År **2025**		År **2026**		År **2027**		**I ALT**	
	Art[93]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[94] Udvikling og gennemførelse af kurser																						
Antal interne kurser	0,34 pr. kursus		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Onlineuddannelse	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Subtotal				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

[93] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[94] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

For at sikre en ensartet gennemførelse og anvendelse af interoperabilitetsløsningerne vil uddannelse blive arrangeret både centralt på EU-plan af Cepol og af medlemsstaterne. Udgifterne til uddannelse på EU-plan omfatter:

- udvikling af fælles læseplan, som medlemsstaterne skal anvende, når de gennemfører national uddannelse

- interne aktiviteter til uddannelse af underviserne. I de to år umiddelbart efter interoperabilitetsløsningerne idriftsættes, forventes uddannelsen at blive gennemført i større målestok og senere vedligeholdt af to interne kurser om året.

- onlinekursus til at supplere de interne aktiviteter på EU-plan og i medlemsstaterne.

3.2.2.4. Anslåede virkninger på eu-LISA's bevillinger

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater **eu-LISA** ⇩			År **2019**		År **2020**		År **2021**		År **2022**		År **2023**		År **2024**		År **2025**		År **2026**		År **2027**		**I ALT**	
	Art[95]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[96] Udvikling af interoperabilitetskomponenter																						
Byggede systemer	Kontrahent			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Softwareprodukter	Software			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Hardwareprodukter	Metalprodukter			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
It-uddannelse	Uddannelse og andet			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340

[95] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[96] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

Subtotal for specifikt mål nr. 1		**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Dette mål omfatter kun udgifterne til levering af de fire interoperabilitetskomponenter og CRRS.

– Omkostningerne til den fælles BMS er blevet anslået med den forudsætning, at ind- og udrejsesystemet, som er ved at blive udviklet, vil fungere som det centrale system til udviklingen. Det er derfor planen at genbruge de biometriske softwarelicenser (36 mio. EUR), som er omfattet til ind- og udrejsesystemet.

– I dette budget behandles den fælles BMS budgetmæssigt som en yderligere udvidelse af BMS til ind- og udrejsesystemet. Den nuværende finansieringsoversigt omfatter derfor marginale omkostninger til softwarelicenser (6,8 mio. EUR) til tilføjelse af ca. 20 mio. biometriske datasæt i SIS AFIS (AFIS er det elektroniske fingeraftryksidentifikationssystem = "BMS" for SIS), Eurodac AFIS og det kommende ECRIS-TCN (det europæiske informationssystem vedrørende strafferegistre for tredjelandsstatsborgere) til BMS leveret til ind- og udrejsesystemet. Omkostningerne til at integrere de forskellige systemer (SIS, Eurodac, ECRIS-TCN) til den fælles BMS er inkluderet i denne finansieringsoversigt.

– Som en del af arbejdet i 2019 og 2020 vil eu-LISA blive bedt om at finde ud af en præcis teknisk løsning, som ikke kan defineres på tidspunktet for indsendelsen af forslaget, samt anslå de omkostningsmæssige konsekvenser af gennemførelsen af den foretrukne tekniske løsning. Dette kan kræve en ændring af de heri forudsatte omkostningsoverslag.

– Alle komponenter leveres inden udgangen af 2023, hvilket forklarer, hvorfor kontrahentens udgifter reduceres til næsten nul på dette tidspunkt. Tilbage er kun et resterende beløb til løbende opdatering af CRRS.

– I perioden 2019-2021 stiger udgifterne til software væsentligt, da omkostningerne til softwarelicenser afholdes for de forskellige miljøer, der er nødvendige til produktion, forproduktion og test, og dette både centralt og alternativt. Desuden prissættes visse specifikke og uundværlige softwarekomponenter i forhold til antallet "refererede objekter" (dvs. mængden af data). Da databasen i sidste ende kommer til at indeholde ca. 220 mio. identiteter, står softwareprisen i rimeligt forhold til denne værdi.

Angiv mål og resultater eu-LISA ⇩			År 2019		År 2020		År 2021		År 2022		År 2023		År 2024		År 2025		År 2026		År 2027		I ALT	
	Art[97]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 2 Vedligeholdelse og drift af interoperabilitetskomponenter																						
Systemer i drift	Kontrahent			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Softwareprodukter	Software			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Hardwareprodukter	Metalprodukter			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
It-uddannelse	Uddannelse			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Subtotal for specifikt mål nr. 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– Vedligeholdelsen starter, så snart nogle komponenter er leveret. Derfor er budgettet for en vedligeholdelseskontrahent inkluderet fra det tidspunkt, hvor ESP leveres (i 2021). Vedligeholdelsesbudgettet stiger i takt med, at flere komponenter leveres, og når derefter en mere eller mindre konstant værdi, der repræsenterer en procentdel (mellem 15 og 22 %) af den oprindelige investering.

[97] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

– Vedligeholdelse af hardware og software starter fra året for idriftsættelsen: Udviklingen i omkostningerne svarer til udviklingen i kontrahentens omkostninger.

Angiv mål og resultater eu-LISA ⇩			År 2019		År 2020		År 2021		År 2022		År 2023		År 2024		År 2025		År 2026		År 2027		I ALT	
	Art[98]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 3[99] Datamigration																						
Oprindelige data fra BMS	Til fælles BMS			0		0		0		7,000		3,000		0		0		0		0		10,000
Gamle EDAC-data til migration	Nyt design og ombygning af EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Subtotal for specifikt mål nr. 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– For så vidt angår den fælles BMS, skal data migreres fra andre biometriske systemer til den fælles BMS, da dette fælles system driftsmæssigt er mere effektivt og også giver en økonomisk fordel i forhold til en situation, hvor der fortsat vil blive opretholdt flere mindre BMS-systemer.

– Den nuværende forretningslogik i Eurodac adskiller sig ikke klart fra den fælles biometriske matchtjeneste, ligesom det er tilfældet med den BMS, der opererer med VIS. Den interne funktion i Eurodac og den mekanisme, hvormed forretningstjenesten kalder de underliggende biometriske matchtjenester, er en sort boks til den eksterne fremviser og er baseret på egen teknologi. Det vil ikke være muligt blot at migrere

[98] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[99] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

data til en fælles BMS og bibeholde det eksisterende forretningslag. Datamigrationen er derfor forbundet med betydelige omkostninger til ændring af udvekslingsmekanismerne med Eurodacs centrale applikation.

Angiv mål og resultater eu-LISA ⇩			År 2019		År 2020		År 2021		År 2022		År 2023		År 2024		År 2025		År 2026		År 2027		I ALT	
	Art[100]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 4[101] Netværk																						
Netværksforbindelser	Netværksopsætning			0		0		0		0,505										0		0,505
Håndteret netværkstrafik	Netværksdrift			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Subtotal for specifikt mål nr. 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– Interoperabilitetskomponenterne har kun en marginal effekt på netværkstrafikken. Med hensyn til data oprettes der kun links mellem eksisterende data, hvilket er et lavvolumenelement. Omkostningerne omfatter her kun den marginale stigning i budgettet, som er krævet oven i budgettet for ind- og udrejsesystemet og ETIAS til netværksopsætning og trafik.

[100] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).
[101] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

Angiv mål og resultater eu-LISA ⇩			År 2019		År 2020		År 2021		År 2022		År 2023		År 2024		År 2025		År 2026		År 2027		I ALT	
	Art[102]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 5[103] Opdatering af national ensartet grænseflade																						
National ensartet grænseflade	Kontrahent			0		0		0		0,505		0,505								0		1,010
Subtotal for specifikt mål nr. 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– Forslaget om ind- og udrejsesystemet indførte begrebet med den nationale ensartede grænseflade, som skal udvikles og vedligeholdes af eu-LISA. Ovenstående tabel indeholder budgettet for opdatering af den nationale ensartede grænseflade med en ekstra type informationsudveksling. Der er ingen ekstraomkostninger til driften af den nationale ensartede grænseflade, som der allerede var budgetteret med i forslaget om ind- og udrejsesystemet.

[102] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).
[103] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

Angiv mål og resultater eu-LISA ⇩			År 2019		År 2020		År 2021		År 2022		År 2023		År 2024		År 2025		År 2026		År 2027		I ALT	
	Art 104	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 6: Møder og uddannelse																						
Månedlige statusmøder (Udvikling)	0,021 pr. møde x 10 pr. år		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Kvartalsmøder (drift)	0,021 x 4 pr. år		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Rådgivende grupper	0,021 x 4 pr. år		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
MS-uddannelse	0,025 pr. uddannelse		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Subtotal for specifikt mål nr.			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	1	**0,318**	1	**0,318**	1	**0,318**		**3,502**

[104] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

6												4		4		4		

– Subtotal 6 omfatter udgifter til afholdelse af møder med forvaltningsmyndigheden (i dette tilfælde eu-LISA) om projektstyring. Det er omkostninger til ekstra møder om levering af interoperabilitetskomponenterne.

– Subtotal 6 omfatter udgifter til møder mellem eu-LISA og medlemsstatens medarbejdere, der beskæftiger sig med udvikling, vedligeholdelse og drift af interoperabilitetskomponenterne og med at tilrettelægge og gennemføre uddannelse af medlemsstaternes it-medarbejdere.

– I udviklingsfasen omfatter budgettet 10 projektmøder om året. Når driften skal forberedes (og dette gælder for 2019 og fremefter), afholdes der fire møder om året. På et mere overordnet plan oprettes der fra starten en rådgivende gruppe, som skal gennemføre Kommissionens gennemførelsesafgørelser. Der er planlagt fire møder om året ligesom for de eksisterende rådgivende grupper. Endvidere forbereder og gennemfører eu-LISA uddannelse af it-medarbejdere i medlemsstaterne. Det er uddannelse i interoperabilitetskomponenternes tekniske aspekter.

Angiv mål og resultater eu-LISA ⇩			År 2019		År 2020		År 2021		År 2022		År 2023		År 2024		År 2025		År 2026		År 2027		I ALT	
	Art[105]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 7[106] Høj tilgængelighed af ECRIS-TCN																						
System med høj tilgængelighed	Systemopsætning			0		0		8,067												0		8,067
Drift med høj tilgængelighed	Systemvedligeholdelse og drift			0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Subtotal for specifikt mål nr. 4				**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– Mål nr. 7 er at flytte ECRIS-TCN fra et system med "standardtilgængelighed" til et system med høj tilgængelighed. I 2021 gennemgår ECRIS-TCN en opgradering, som kræver, at der indkøbes yderligere hardware. Eftersom det er planen, at ECRIS-TCN skal være afsluttet i 2020, er det fristende at opbygge dette system som et system med høj tilgængelighed fra starten og integrere det med interoperabilitetskomponenterne. Men i betragtning af at mange projekter bliver afhængige af hinanden, er det fornuftigt ikke at gøre denne antagelse og budgettere med særskilte foranstaltninger. Dette budget kommer ud over omkostningerne til udvikling, vedligeholdelse og drift af ECRIS-TCN i 2019 og 2020.

[105] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).
[106] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

3.2.2.5. Anslåede virkninger for GD Homes bevillinger

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater **GD Home** ⇩			År **2019**		År **2020**		År **2021**		År **2022**		År **2023**		År **2024**		År **2025**		År **2026**		År **2027**		**I ALT**	
	Art[107]	Gennemsnitlige omkostninger	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal	Omkostning	Antal i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1: Integration af (medlemsstaternes) nationale systemer																						
National ensartet grænseflade klar til brug	Tilpasning af national ensartet grænseflade – udvikling						30	3,150	30	3,150											30	6,300
MS-systemer tilpasset til interoperabilitet	Integrationsomkostninger						30	40,000	30	40,000	30	40,000									30	120,000

[107] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

Slutbrugeruddannelse	10 000 slutbrugersessioner i alt à 1 000 EUR pr. session							5000	5,000	5000	5,000								10,000	10,000
Subtotal for specifikt mål nr. 1							**43,150**		**48,150**		**45,000**									**136,300**

– Specifikt mål nr. 1 omhandler de midler, der stilles til medlemsstaternes rådighed, så de kan udnytte fordelene ved de interoperable centrale systemer. Den nationale ensartede grænseflade tilpasses, både når ESP gennemføres, og når MID idriftsættes. Hver medlemsstat skal indføre en relativt moderat ændring (anslået til 150 mandedage) for at tilpasse sig disse opdaterede meddelelsesudvekslinger med de centrale systemer. Mere omfattende er ændringen i indholdet af de data, som interoperabilitet medfører, og som er omfattet af "integrationsomkostninger". Disse midler omfatter ændringer i de meddelelser, der sendes til det centrale system, og i håndteringen af svarene. Til vurdering af omkostningerne ved disse ændringer bevilges et budget på 4 mio. EUR pr. medlemsstat. Dette beløb er det samme som for ind- og udrejsesystemet, eftersom det kræver en tilsvarende mængde arbejde at tilpasse integrationen af de nationale systemer med den nationale ensartede grænseflade.

– Slutbrugerne skal uddannes i systemerne. Denne uddannelse af en meget stor gruppe af slutbrugere skal finansieres på grundlag af 1 000 EUR pr. session for 10 til 20 slutbrugere for de anslåede 10 000 sessioner, som skal tilrettelægges af alle medlemsstaterne i egne lokaler.

3.2.3. Anslåede virkninger for administrationsbevillingerne

3.2.3.1. Sammendrag af Det Europæiske Agentur for Grænse- og Kystbevogtning

☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

☒ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
Tjenestemænd (AD)										
Tjenestemænd (AST)	0									
Kontraktansat personale	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Midlertidigt ansatte	0	0	0	0	0	0	0	0	0	0
Udstationerede nationale eksperter										
I ALT	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

Det forventede arbejde, der skal udføres af disse ekstra medarbejdere i Det Europæiske Agentur for Grænse- og Kystbevogtning, er tidsbegrænset (2023) og starter mere præcist, 24 måneder efter den biometriske søgemaskine til ind- og udrejsesystemet bliver tilgængelig). Medarbejderne skal dog være ansat på forhånd (gennemsnitligt tre måneder), hvilket forklarer værdien i 2022. Det udførte arbejde efterfølges af afsluttende opgaver i to måneder, hvilket forklarer personaleniveauet i 2024.

Personaleniveauet er baseret på de 20 personer, der kræves for at udføre arbejdet (plus 10 personer, som en kontrahent stiller til rådighed, og som afspejles i afsnit 3). Opgaver ventes endvidere at blive udført over udvidede arbejdstimer og ikke begrænset til standardarbejdstid. Støttepersonale og ledende medarbejdere antages at blive hentet fra agenturets ressourcer.

Antallet af medarbejdere er baseret på den antagelse, at der skal vurderes ca. 550 000 fingeraftryk, hvilket tager i gennemsnit 5-10 minutter pr. sag (17 000 aftryk pr. år)[108].

[108] Medarbejderstaben i 2020 og derefter er vejledende og skal vurderes, uanset om dette kommer oven i prognosen om Det Europæiske Agentur for Grænse- og Kystbevogtnings personale som fastsat i COM(2015)671 eller ej.

Number of staff	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Staff for processing links and decisions manually	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Title 1 - CA	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Title 1 - TA	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Total Title 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

.

3.2.3.2. Sammendrag af Europol

☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

☒ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
Tjenestemænd (AD)										
Tjenestemænd (AST)	0									
Kontraktansat personale	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Midlertidigt ansatte	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Udstationerede nationale eksperter										
I ALT	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Disse udgifter er anslået på grundlag af følgende personaleniveauer:

Antal fuldtidsækvivalenter for IKT	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**I alt**
Kontraktansat personale	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Midlertidigt ansatte	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Personale i alt (FTÆ)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Der ventes at blive ansat yderligere IT-personale i Europol for at styrke Europols informationssystemer, så de kan håndtere det øgede antal forespørgsler fra ESP og ETIAS og senere vedligeholde systemerne 24/7.

– I gennemførelsesfasen for ESP (i 2020 og 2021) er der et yderligere behov for tekniske eksperter (arkitekter, ingeniører, udviklere, testere). Der er behov for færre tekniske eksperter i 2022 og fremefter til at gennemføre resten af interoperabilitetskomponenterne og vedligeholde systemerne.

– Fra anden halvdel af 2021 skal der gennemføres 24/7-overvågning af IKT-systemerne for at sikre serviceniveauer for ESP og ETIAS. Dette gøres af to kontraktansatte, der arbejder i fire skift 24/7.

– I videst muligt omfang er profilerne delt mellem midlertidigt ansatte og kontraktansatte. Det skal dog bemærkes, at på grund af høje sikkerhedskrav er det i flere stillinger kun muligt at bruge midlertidigt ansatte. I anmodningen om midlertidigt ansatte tages der hensyn til resultaterne af forligsproceduren om 2018-budgettet.

3.2.3.3. Sammendrag af Cepol

☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

☒ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
Tjenestemænd (AD)										
Tjenestemænd (AST)										
Kontraktansat personale			0,070	0,070						**0,140**
Midlertidigt ansatte		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Udstationerede nationale eksperter										
I ALT		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Der er brug for ekstra personale, da uddannelse af medlemsstaternes undervisere skal udvikles, specielt med henblik på at anvende interoperabilitetskomponenterne i driftsmæssige sammenhænge.

- Udvikling af læseplaner og uddannelsesmoduler skal starte mindst otte måneder, før systemet idriftsættes. I de første to år efter idriftsættelsen er uddannelsen mest intensiv. Den

skal dog opretholdes i en længere periode til at sikre en sammenhængende gennemførelse baseret på erfaringerne med Schengeninformationssystemet.

- Det ekstra personale er nødvendigt for at udarbejde, koordinere og gennemføre læseplan, interne kurser og onlinekurser. Disse kurser kan kun gennemføres ud over Cepols eksisterende uddannelseskatalog, og der er derfor behov for ekstra personale.

- Planen er at have én kursusleder som midlertidigt ansat i hele udviklings- og vedligeholdelsesperioden, som vil blive støttet af en kontraktansat i den mest intensive periode med tilrettelæggelse af uddannelsen.

3.2.3.4. Sammendrag af eu-LISA

☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

☒ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
Tjenestemænd (AD)										
Tjenestemænd (AST)										
Kontraktansat personale	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Midlertidigt ansatte	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Udstationerede nationale eksperter										
I ALT	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– I personalebehovet tages der højde for, at de fire komponenter og CRRS udgør en portefølje af indbyrdes afhængige projekter (dvs. et program). For at styre afhængigheder mellem projekter oprettes der et programstyringsteam bestående af program- og projektledere og profiler (ofte omtalt som arkitekter), der skal definere de fælles indbyrdes elementer. Programmets/projektets realisering kræver også profiler til program- og projektsupport.

– Personalebehovet pr. projekt er blevet anslået analogt med tidligere projekter (visuminformationssystemet) og skelner mellem projektets færdiggørelse og driftsfasen.

– De profiler, som skal blive under driftsfasen, ansættes som midlertidigt ansatte. De profiler, som skal bruges til programmets/projektets udførelse, ansættes som kontraktansatte. For at sikre den forventede kontinuitet af opgaver og for at holde viden

inden for agenturet fordeles antallet af stillinger næsten 50/50 på midlertidigt ansatte og kontraktansatte.

– Det antages, der ikke vil være behov for yderligere personale til at gennemføre ECRIS-TCN projektet med høj tilgængelighed, og at eu-LISA's projektmedarbejdere vil bestå af eksisterende medarbejdere fra projekter, der afsluttes omkring dette tidspunkt.

Disse estimater er baseret på de følgende personaleniveauer:

For kontraktansat personale:

3.2.1. outputs EU-LISA (is equal to T1) in number of persons	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total (formula)
Contract Staff										-
Programme/project mgt	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS PM	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Programme/project office	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Quality Assurance	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Financial and Procurement	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Financial mgt										*0,0*
Budgetary planning and control										*0,0*
Procurement/contract mgt	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Technical experts	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Shared BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Testing	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Shared BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
System monitoring	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Common (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
General Coordination	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Human resources	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Sub- total Contract Staff	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

For midlertidigt ansatte:

Temporary staff										
Programme/project mgt	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Programme mgr	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Project mgt	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Programme/project office	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
Shared BMS	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Financial and Procurement	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Financial mgt	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Budgetary planning and control	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Procurement/contract mgt	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Technical experts	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Shared BMS	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Security	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architects	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Testing	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
Shared BMS	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
System monitoring	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Shared BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Training	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Training	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Human resources	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Other	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Data protection specialist	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Sub-total Temporary Agents	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Total	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Anslåede virkninger for administrationsbevillingerne

3.2.4.1. GD Home: Sammendrag

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**	**I ALT**
UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme										
Menneskelige ressourcer DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Andre administrationsudgifter	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Subtotal UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Uden for UDGIFTSOMRÅDE 5[109] i den flerårige finansielle ramme	(Ikke anvendt)									
Menneskelige ressourcer										
Andre udgifter af administrativ art										
Subtotal uden for UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme										

I ALT	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

[109] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller aktioner (tidligere BA-poster), indirekte forskning, direkte forskning.

.

3.2.4.2. Anslåede behov for personaleressourcer

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– ☒ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i fuldtidsækvivalenter

		År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	I ALT
• **Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)**											
18 01 01 01 (i hovedsædet og i Kommissionens repræsentationskontorer) DG HOME		5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (delegationer)											
XX 01 05 01 (indirekte forskning)											
10 01 05 01 (direkte forskning)											
•**Eksternt personale (fuldtidsækvivalenter: FTÆ)**[110]											
XX 01 02 02 (KA, LA, UNE, V og JED i delegationerne)											
XX 01 04 **yy** 111	- ved hovedsædet										
	- i delegationerne										
XX 01 05 02 (KA, UNE, V – indirekte forskning)											
10 01 05 02 (KA, UNE, V – direkte forskning)											
Andre budgetposter (specificer)											
I ALT		**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til aktionen, og/eller interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Opgavebeskrivelse:

Projektovervågning og -opfølgning. Tre embedsmænd til opfølgning. Personalet beskæftiger sig med at tage Kommissionens opgaver op i forbindelse med levering af programmet: kontrol af overholdelsen af forslaget, besvarelse af spørgsmål om overholdelse, udarbejdelse af rapporter til Europa-Parlamentet og Rådet, vurdering af status i medlemsstaternes. Da programmet er en ekstra aktivitet sammenlignet med eksisterende arbejdsbyrder, er ekstra personale påkrævet. Denne personalestigning er begrænset i varighed og dækker kun udviklingsperioden.

Forvaltning af UMF

[110] KA: kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JED= junioreksperter ved delegationerne.

[111] Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

Kommissionen forvalter UMF-standarden på daglig basis. Dette kræver to embedsmænd: en person som retshåndhævelsesekspert og en anden med godt kendskab til forretningsmodeller og IKT-viden.

Det universelle meddelelsesformat (UMF) fastsætter en standard for struktureret, grænseoverskridende informationsudveksling mellem informationssystemer, myndigheder og/eller organisationer på området for retlige og indre anliggender. UMF definerer et fælles sprogbrug og logiske strukturer for almindeligt udvekslede oplysninger med det formål at lette interoperabiliteten ved at gøre det muligt at oprette og læse indholdet af udvekslingen på en sammenhængende og semantisk ensartet måde.

For at sikre ensartede betingelser for gennemførelsen af det universelle meddelelsesformat foreslås det at tillægge Kommissionen gennemførelsesbeføjelser. Disse beføjelser foreslås udøvet i overensstemmelse med 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.

3.2.5. Forenelighed med den nuværende flerårige finansielle ramme

– ☐ Forslaget/initiativet er foreneligt med indeværende og næste flerårige finansielle ramme

– ☒ Forslaget/initiativet kræver omlægning af det relevante udgiftsområde i den flerårige finansielle ramme

Der redegøres for omlægningen med angivelse af de berørte budgetposter og beløbenes størrelse.

Forordningen om Fonden for Intern Sikkerhed (ISF) er det finansielle instrument, hvor budgettet for gennemførelsen af interoperabilitetsinitiativet indgår.

Den bestemmer i artikel 5, litra b), at 791 mio. EUR skal anvendes til gennemførelsen af et program til udvikling af it-systemer baseret på eksisterende og/eller nye it-systemer til forvaltning af migrationsstrømme på tværs af Unionens ydre grænser, med forbehold af vedtagelsen af de relevante lovgivningsmæssige EU-retsakter og på de betingelser, der er fastsat i artikel 15, stk. 5. Af disse 791 mio. EUR er 480,2 mio. EUR afsat til udvikling af ind- og udrejsesystemet, 210 mio. EUR til ETIAS og 67,9 mio. EUR til revision af SIS II. Den resterende del (32,9 mio. EUR) omfordeles ved hjælp af ISF-B-mekanismer. **Det nuværende forslag kræver 32,1 mio. EUR for den nuværende FFR-periode, hvilket passer med det resterende budget**.

Konklusionen i boksen ovenfor om det krævede beløb på 32,1 mio. EUR er resultatet af følgende beregning:

COMMITMENTS										
3.2. Estimated impact on expenditure DG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (horiz)**
18 02 01 03 - Smart Borders (covers the support to MS)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Total (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formula)**
T1: Staff expenditures	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: Infrastructure and Operating Expenditure	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Operational Expenditure	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Total (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Staff expenditures	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Infrastructure and Operating Expenditure	0	0	0	0	0	0	0	0	0	0
T3: Operational Expenditure	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Total (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18.02.05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Staff expenditures	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Infrastructure and Operating Expenditure	0	0	0	0	0	0	0	0	0	0
T3: Operational Expenditure	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Total (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex - EBCG										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Staff expenditures	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: Infrastructure and Operating Expenditure	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: Operational Expenditure	0	0	0	0,183	2,200	0	0	0	0	2,383
Total (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
TOTAL (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. DG HOME Heading 5 'Administrative expenditure'										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Total (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTAL (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ Forslaget/initiativet kræver, at fleksibilitetsinstrumentet anvendes, eller at den flerårige finansielle ramme revideres.

3.2.6. Tredjemands bidrag til finansieringen

– Forslaget/initiativet indeholder **ikke** bestemmelser om samfinansiering med tredjeparter.

3.3. Anslåede virkninger for indtægterne

– ☐ Forslaget/initiativet har ingen finansielle virkninger for indtægterne.

– ☒ Forslaget/initiativet har følgende finansielle virkninger:

– – ☐ for egne indtægter

– – ☒ for diverse indtægter

i mio. EUR (tre decimaler)

Indtægtspost på budgettet:	Bevillinger til rådighed i indeværende regnskabsår	Forslagets/initiativets virkninger[112]								
		År **2019**	År **2020**	År **2021**	År **2022**	År **2023**	År **2024**	År **2025**	År **2026**	År **2027**
Artikel 6313 - Bidrag fra associerede Schengenlande (CH, NO, LI, IS).....		pm	pm	pm	pm	pm	pm	pm	pm	pm

For diverse indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der påvirkes.

18,0207

Det oplyses, hvilken metode der er benyttet til at beregne virkningerne for indtægterne.

Budgettet vil omfatte bidrag fra lande, der er associeret med gennemførelsen, anvendelsen og udviklingen af Schengenreglerne og Eurodac-relaterede foranstaltninger, således som det er fastsat i de respektive aftaler.

[112] Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 25 %.