DEN EUROPÆISKE UNION

EUROPA-PARLAMENTET **RÅDET**

Strasbourg, den 13. marts 2024
(OR. en)

2021/0410(COD)
LEX 2301

PE-CONS 75/1/23
REV 1

IXIM 237
ENFOPOL 525
JAI 1599
CODEC 2358

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING OM AUTOMATISERET SØGNING OG UDVEKSLING AF DATA MED HENBLIK PÅ POLITISAMARBEJDE, OG OM ÆNDRING AF RÅDETS AFGØRELSE 2008/615/RIA OG 2008/616/RIA OG EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2018/1726, (EU) 2019/817 OG (EU) 2019/818 (PRÜM II-FORORDNINGEN)

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2024/…

af 13. marts 2024

om automatiseret søgning og udveksling af data med henblik på politisamarbejde, og om ændring af Rådets afgørelse 2008/615/RIA og 2008/616/RIA og Europa-Parlamentets og Rådets forordning (EU) 2018/1726, (EU) 2019/817 og (EU) 2019/818 (Prüm II-forordningen)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16, stk. 2, artikel 87, stk. 2, litra a), og artikel 88, stk. 2,

under henvisning til forslag fra Europa-Kommissionen,

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

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

efter den almindelige lovgivningsprocedure[2], og

ud fra følgende betragtninger:

---

1 EUT C 323 af 26.8.2022, s. 69.

2 Europa-Parlamentets holdning af 8.2.2024 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 26.2.2024.

(1) Unionen har sat sig det mål at sikre borgerne et område med frihed, sikkerhed og retfærdighed uden indre grænser, hvor der er fri bevægelighed for personer. Dette mål skal nås ved hjælp af blandt andet passende foranstaltninger for at forebygge og bekæmpe kriminalitet og andre trusler mod den offentlige sikkerhed, herunder organiseret kriminalitet og terrorisme, i overensstemmelse med Kommissionens meddelelse af 24. juli 2020 om strategien for EU's sikkerhedsunion. Dette mål kræver, at de retshåndhævende myndigheder udveksler data på en effektiv og rettidig måde for effektivt at forebygge, afsløre og efterforske strafbare handlinger.

(2) Denne forordnings mål er derfor, med henblik på at forebygge, afsløre og efterforske strafbare handlinger, at forbedre, strømline og lette udvekslingen af strafferetlige oplysninger og køretøjsregistreringsdata mellem medlemsstaternes kompetente myndigheder og mellem medlemsstater og Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol), oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2016/794[3], i fuld overensstemmelse med grundlæggende rettigheder og databeskyttelsesregler.

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

(3) Rådets afgørelse 2008/615/RIA[4] og 2008/616/RIA[5], der fastlægger regler for udveksling af oplysninger mellem myndigheder med ansvar for forebyggelse og efterforskning af strafbare handlinger ved at give mulighed for elektronisk overførsel af DNA-profiler, fingeraftryksoplysninger og visse oplysninger fra køretøjsregistre har vist sig at være vigtige for bekæmpelse af terrorisme og grænseoverskridende kriminalitet, hvorved indre sikkerhed for Unionen og dens borgere beskyttes.

---

[4] Rådets afgørelse 2008/615/RIA af 23. juni 2008 om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (EUT L 210 af 6.8.2008, s. 1).

[5] Rådets afgørelse 2008/616/RIA af 23. juni 2008 om gennemførelse af afgørelse 2008/615/RIA om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (EUT L 210 af 6.8.2008, s. 12).

(4) Denne forordning bør på grundlag af eksisterende procedurer for automatiseret søgning efter oplysninger fastsætte betingelserne og procedurerne for automatiseret søgning og udveksling af DNA-profiler, fingeraftryksdata, køretøjsregistreringsdata, visse kørekortdata, ansigtsbilleder og politiregistre. Dette bør ikke berøre behandlingen af sådanne data i Schengeninformationssystemet (SIS) eller udvekslingen af supplerende oplysninger med forbindelse til sådanne data via Sirene-kontorerne i medfør af Europa-Parlamentets og Rådets forordning (EU) 2018/1862[6] eller rettighederne for personer, hvis data behandles deri.

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

(5) Denne forordning fastlægger en ramme for udveksling af oplysninger mellem myndigheder med ansvar for forebyggelse, afsløring og efterforskning af strafbare handlinger (Prüm II-rammen). I overensstemmelse med artikel 87, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde (TEUF) omfatter den alle medlemsstaternes kompetente myndigheder, herunder, men ikke begrænset til politi, toldmyndigheder og andre særlige retshåndhævende myndigheder inden for forebyggelse, afsløring og efterforskning af strafbare handlinger. I forbindelse med denne forordning bør enhver myndighed, der er ansvarlig for forvaltningen af en national database, der er omfattet af denne forordning, eller som giver en retskendelse til at frigive data, derfor anses for at være omfattet af denne forordnings anvendelsesområde, så længe oplysninger udveksles med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger.

(6) Enhver behandling eller udveksling af personoplysninger med henblik på denne forordning bør ikke føre til forskelsbehandling af personer af nogen grunde. Den bør fuldt ud respektere menneskelig værdighed og integritet og andre grundlæggende rettigheder, herunder retten til respekt for privatlivet og til beskyttelse af personoplysninger, i overensstemmelse med Den Europæiske Unions charter om grundlæggende rettigheder.

(7) Enhver behandling eller udveksling af personoplysninger bør være omfattet af reglerne om databeskyttelse i denne forordnings kapitel 6 og, alt efter hvad der er relevant, Europa-Parlamentets og Rådets direktiv (EU) 2016/680[7] eller Europa-Parlamentets og Rådets forordning (EU) 2018/1725[8], (EU) 2016/794 eller (EU) 2016/679[9]. Direktiv (EU) 2016/680 finder anvendelse på brugen af Prüm II-rammen i forbindelse med søgninger efter forsvundne personer og identifikation af uidentificerede menneskelige rester med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger, mens forordning (EU) 2016/679 finder anvendelse på brugen af Prüm II-rammen i forbindelse med søgninger efter forsvundne personer og identifikation af uidentificerede menneskelige rester for andre formål.

---

7 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).

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

9 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 (den generelle forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

(8) Ved at fastsætte bestemmelser om automatiseret søgning efter DNA-profiler, fingeraftryksdata, visse køretøjsregistreringsdata, ansigtsbilleder og politiregistre er formålet med denne forordning også at gøre det muligt at søge efter forsvundne personer og identificere uidentificerede menneskelige rester. Disse automatiserede søgninger bør følge de regler og procedurer, der er fastsat i denne forordning. Disse automatiserede søgninger berører ikke indlæsningen af indberetninger om forsvundne personer i SIS og udvekslingen af supplerende oplysninger om sådanne indberetninger i henhold til forordning (EU) 2018/1862.

(9) Hvor medlemsstaterne ønsker at anvende Prüm II-rammen til at søge efter forsvundne personer og identificere menneskelige rester, bør de vedtage nationale lovgivningsmæssige foranstaltninger til at udpege de nationale myndigheder, der er kompetente til dette formål, og fastsætte de specifikke procedurer, betingelser og kriterier til dette formål. For så vidt angår søgninger efter forsvundne personer uden for området strafferetlig efterforskning bør de nationale lovgivningsmæssige foranstaltninger klart fastsætte de humanitære årsager, på grundlag af hvilke der kan foretages en søgning efter forsvundne personer. Sådanne søgninger bør overholde proportionalitetsprincippet. De humanitære årsager bør omfatte naturkatastrofer og menneskeskabte katastrofer og andre lige så velbegrundede årsager, såsom mistanke om selvmord.

(10) Ved denne forordning fastsættes betingelserne og procedurerne for automatiseret søgning efter DNA-profiler, fingeraftryksdata, visse køretøjsregistreringsdata, ansigtsbilleder og politiregistre og reglerne for udveksling af centrale data efter et bekræftet match mellem biometriske data. Den finder ikke anvendelse på udveksling af supplerende oplysninger ud over, hvad der er fastsat i denne forordning, som reguleres af Europa-Parlamentets og Rådets direktiv (EU) 2023/977[10].

(11) Direktiv (EU) 2023/977 udgør en sammenhængende EU-retlig ramme for at sikre, at en medlemsstats kompetente myndigheder har lige adgang til oplysninger, som andre medlemsstater er i besiddelse af, når de har brug for sådanne oplysninger til at bekæmpe kriminalitet og terrorisme. For at forbedre udvekslingen af oplysninger formaliserer og præciserer nævnte direktiv reglerne og procedurerne for udveksling af oplysninger mellem medlemsstaternes kompetente myndigheder, navnlig med henblik på efterforskning, herunder den rolle, som hver medlemsstats centrale kontaktpunkt spiller for sådanne udvekslinger.

(12) Formålene med udveksling af DNA-profiler i henhold til denne forordning berører ikke medlemsstaternes enekompetence til at beslutte formålet med deres nationale DNA-databaser, herunder forebyggelse eller afsløring af strafbare handlinger.

---

[10] Europa-Parlamentets og Rådets direktiv (EU) 2023/977 af 10. maj 2023 om udveksling af oplysninger mellem medlemsstaternes retshåndhævende myndigheder og om ophævelse af Rådets rammeafgørelse 2006/960/RIA (EUT L 134 af 22.5.2023, s. 1).

(13) Medlemsstaterne bør på det tidspunkt, hvor der første gang etableres forbindelse til routeren oprettet ved denne forordning, foretage automatiserede søgninger ved at sammenligne alle DNA-profilerne lagret i deres databaser med alle DNA-profilerne lagret i alle de andre medlemsstaters databaser og i Europoldata. Formålet med denne første automatiserede søgning er at undgå huller i identifikationen af match mellem DNA-profiler lagret i en medlemsstats database og DNA-profiler lagret i alle de andre medlemsstaters databaser og i Europoldata. Den første automatiserede søgning bør foretages bilateralt og bør ikke nødvendigvis udføres med alle andre medlemsstaters databaser og Europoldata samtidig. Ordningerne for at foretage sådanne søgninger, herunder tidsplanen og mængden pr. batch, bør aftales bilateralt i overensstemmelse med de regler og procedurer, der er fastsat i denne forordning.

(14) Efter den første automatiserede søgning af DNA-profiler bør medlemsstaterne foretage automatiserede søgninger ved at sammenligne alle de nye DNA-profiler, der er tilføjet til deres databaser, med alle de DNA-profiler, som er lagret i alle andre medlemsstaters databaser og i Europoldata. Denne automatiserede søgning efter nye DNA-profiler bør finde sted regelmæssigt. Hvor sådanne søgninger ikke kan finde sted, bør den berørte medlemsstat have mulighed for at foretage dem på et senere tidspunkt for at sikre, at ingen match bliver overset. Ordningerne for sådanne senere søgninger, herunder tidsplanen og mængden pr. batch, bør aftales bilateralt i overensstemmelse med de regler og procedurer, der er fastsat i denne forordning.

(15) Til automatiseret søgning af køretøjsregistreringsdata bør medlemsstaterne og Europol anvende det europæiske informationssystem vedrørende køretøjer og kørekort (Eucaris), der er oprettet ved traktaten om et europæisk informationssystem vedrørende køretøjer og kørekort (EUCARIS) og er udformet til dette formål, og som forbinder alle deltagende medlemsstater i et netværk. Der er ikke behov for en central komponent for at etablere kommunikationen, da hver medlemsstat kommunikerer direkte med de andre forbundne medlemsstater, og Europol kommunikerer direkte med de forbundne databaser.

(16) Identifikation af en kriminel person er afgørende for en vellykket strafferetlig efterforskning og retsforfølgning. Automatiseret søgning efter ansigtsbilleder af personer, der er dømt eller mistænkt for at have begået en strafbar handling, eller ofre, hvor dette er tilladt i henhold til den anmodede medlemsstats nationale ret, og som er indsamlet i overensstemmelse med national ret, vil kunne give yderligere oplysninger for en vellykket identifikation af kriminelle og bekæmpelse af kriminalitet. I betragtning af de pågældende datas følsomhed bør det kun være muligt at foretage automatiseret søgning med henblik på at forebygge, afsløre eller efterforske en strafbar handling, der kan straffes med en maksimal fængselsstraf på mindst ét år i henhold til den anmodende medlemsstats ret.

(17) Automatiseret søgning efter biometriske data foretaget af medlemsstaternes kompetente myndigheder med ansvar for forebyggelse, afsløring og efterforskning af strafbare handlinger i henhold til denne forordning bør kun vedrøre data i databaser, der er oprettet med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger.

(18) Deltagelse i automatiseret søgning i og udvekslingen af politiregistre bør fortsat være frivillig. Hvor medlemsstater beslutter at deltage, bør det, i en ånd af gensidighed, kun være muligt for dem at foretage forespørgsler i andre medlemsstaters databaser, hvis de stiller deres egne databaser til rådighed for andre medlemsstaters forespørgsler. Deltagende medlemsstater bør oprette nationale politiregisterindekser. Det bør være op til medlemsstaterne at beslutte, hvilke nationale databaser, der er oprettet med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger, de vil anvende til oprettelse af deres nationale politiregisterindekser. Disse indekser omfatter data fra nationale databaser, som politiet sædvanligvis kontrollerer ved modtagelse af anmodninger om oplysninger fra andre retshåndhævende myndigheder. Denne forordning opretter det europæiske politiregisterindekssystem (EPRIS) i overensstemmelse med princippet om indbygget databeskyttelse. Databeskyttelsesgarantier omfatter pseudonymisering, eftersom indekser og forespørgsler ikke indeholder klare personoplysninger, men alfanumeriske strenge. Det er vigtigt, at EPRIS forhindrer medlemsstaterne eller Europol i ud fra pseudonymiseringen at genskabe og afsløre de identifikationsdata, der førte til et match. I betragtning af de pågældende oplysningers følsomhed bør udveksling af nationale politiregisterindekser i henhold til denne forordning kun vedrøre dataene om personer, der er dømt eller mistænkt for at have begået en strafbar handling. Desuden bør det kun være muligt at foretage automatiseret søgning med henblik på at forebygge, afsløre eller efterforske en strafbar handling, der kan straffes med en maksimal fængselsstraf på mindst ét i henhold til den anmodende medlemsstats ret.

(19) Udvekslingen af politiregistre i henhold til denne forordning berører ikke udvekslingen af strafferegistre gennem det eksisterende europæiske informationssystem vedrørende strafferegistre (ECRIS), der blev oprettet ved Rådets rammeafgørelse 2009/315/RIA[11].

(20) I de senere år har Europol modtaget en stor mængde biometriske data om personer mistænkt og personer dømt for terrorisme og strafbare handlinger fra tredjelandes myndigheder i overensstemmelse med forordning (EU) 2016/794, herunder kamppladsoplysninger fra krigszoner. I mange tilfælde har det ikke været muligt at udnytte sådanne data fuldt ud, fordi de ikke altid er tilgængelige for medlemsstaternes kompetente myndigheder. Det er nødvendigt at medtage data fra tredjelande, som er lagret af Europol, inden for Prüm II-rammen og dermed stille disse data til rådighed for medlemsstaternes kompetente myndigheder i overensstemmelse med Europols rolle som Unionens centrale knudepunkt for strafferetlige oplysninger, for bedre at forebygge, afsløre og efterforske alvorlige strafbare handlinger. Det bidrager også til at skabe synergier mellem forskellige retshåndhævelsesværktøjer og sikrer, at data anvendes på den mest effektive måde.

[11] Rådets rammeafgørelse 2009/315/RIA af 26. februar 2009 om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne (EUT L 93 af 7.4.2009, s. 23).

(21) Europol bør kunne søge i medlemsstaternes databaser inden for Prüm II-rammen med oplysninger fra tredjelandes myndigheder under fuld overholdelse af de regler og betingelser, der er fastsat i forordning (EU) 2016/794, med henblik på at etablere grænseoverskridende forbindelser mellem straffesager, der henhører under Europols kompetence. At kunne anvende Prümdata ud over andre databaser, der er til rådighed for Europol, vil gøre det muligt at foretage en mere fuldstændig og informeret analyse og derved sætte Europol i stand til at yde bedre støtte til medlemsstaternes kompetente myndigheder med henblik på forebyggelse, afsløringer og efterforskning af strafbare handlinger.

(22) Europol bør sikre, at dets søgningsanmodninger ikke overstiger den søgekapacitet for fingeraftryksdata og for ansigtsbilleder, som medlemsstaterne har anført. I tilfælde af et match mellem data, der anvendes til søgningen, og data, der er lagret i medlemsstaternes databaser, bør det være op til medlemsstaterne at beslutte, hvorvidt de vil give Europol de oplysninger, der er nødvendige for, at det kan udføre sine opgaver.

(23) Forordning (EU) 2016/794 finder i sin helhed anvendelse på Europols deltagelse i Prüm II-rammen. Enhver anvendelse af Europol af data fra tredjelande reguleres af artikel 19 i forordning (EU) 2016/794. Enhver anvendelse af Europol af data indhentet fra automatiserede søgninger i henhold til Prüm II-rammen bør være betinget af samtykke fra den medlemsstat, som leverede dataene og reguleres af artikel 25 i forordning (EU) 2016/794, hvor dataene er overført til tredjelande.

(24) Afgørelse 2008/615/RIA og 2008/616/RIA indeholder bestemmelser om et netværk af bilaterale forbindelser mellem medlemsstaternes nationale databaser. Som følge af denne tekniske arkitektur var hver medlemsstat nødt til at oprette en forbindelse til hver medlemsstat, der deltager i udvekslingerne, hvilket betød mindst 26 forbindelser, pr. datakategori. Routeren og EPRIS vil forenkle Prümrammens tekniske arkitektur og fungere som forbindelsespunkter mellem alle medlemsstater. Routeren bør kræve en enkelt forbindelse pr. medlemsstat i forbindelse med biometriske data. EPRIS bør kræve en enkelt forbindelse pr. deltagende medlemsstat for så vidt angår politiregistre.

(25) Routeren bør tilkobles den europæiske søgeportal, der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2019/817[12] og Europa-Parlamentets og Rådets forordning (EU) 2019/818[13], for at tillade medlemsstaternes kompetente myndigheder og Europol at iværksætte forespørgsler til nationale databaser i henhold til denne forordning samtidig med forespørgsler til det fælles identitetsregister, der er oprettet ved nævnte forordninger, med henblik på retshåndhævelse i overensstemmelse med nævnte forordninger. Nævnte forordninger bør derfor ændres i overensstemmelse hermed. Forordning (EU) 2019/818 bør derudover ændres med henblik på at muliggøre lagring af rapporter og statistikker vedrørende routeren i det centrale register for rapportering og statistik.

---

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

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

(26) Det bør være muligt for referencenumrene for biometriske data at være et foreløbigt referencenummer eller et transaktionskontrolnummer.

(27) Automatiserede fingeraftryksidentifikationssystemer og systemer til genkendelse af ansigtsbilleder anvender biometriske skabeloner, der består af data fra udtræk af karakteristika fra faktiske biometriske prøver. Biometriske skabeloner bør indhentes fra biometriske data, men det bør ikke være muligt at indhente de samme biometriske data fra de biometriske skabeloner.

(28) Routeren bør, hvor den anmodende medlemsstat beslutter det, og hvor det er relevant for typen af biometriske data, rangordne svarene fra den anmodede medlemsstat eller de anmodede medlemsstater eller fra Europol ved at sammenligne de biometriske data, der anvendes til forespørgsler, og de biometriske data, der leveres i svarene fra den anmodede medlemsstat eller de anmodede medlemsstater eller fra Europol.

(29) I tilfælde af et match mellem de data, der anvendes til søgningen, og data i den anmodede medlemsstats eller de anmodede medlemsstaters nationale database, og efter en kvalificeret medarbejder i den anmodende medlemsstat manuelt har bekræftet dette match og efter overførsel af en beskrivelse af kendsgerningerne og en angivelse af den tilgrundliggende lovovertrædelse ved hjælp af den fælles tabel over lovovertrædelser, der er fastsat i en gennemførelsesretsakt, der skal vedtages i henhold til rammeafgørelse 2009/315/RIA, bør den anmodede medlemsstat returnere et begrænset sæt af centrale data i det omfang, sådanne centrale data er tilgængelige. Det begrænsede sæt af centrale data bør returneres via routeren og inden for 48 timer efter at de relevante betingelser er blevet opfyldt, medmindre der kræves en retskendelse i henhold til national ret. Denne frist vil sikre hurtig udveksling af kommunikation mellem medlemsstaternes kompetente myndigheder. Medlemsstaterne bør bevare kontrollen med frigivelsen af dette begrænsede sæt af centrale data. Menneskelig indgriben bør opretholdes på centrale punkter i processen, herunder for beslutningen om at iværksætte en forespørgsel, beslutningen om at bekræfte et match, beslutningen om at fremsætte en anmodning om at modtage sættet af centrale data efter et bekræftet match og beslutningen om at videregive personoplysninger til den anmodende medlemsstat, for at sikre, at centrale data ikke vil blive udvekslet på en automatiseret måde.

(30) Drejer det sig specifikt om DNA, bør den anmodede medlemsstat også kunne bekræfte et match mellem to DNA-profiler, hvor dette er relevant for efterforskning af strafbare handlinger. Efter den anmodede medlemsstats bekræftelse af dette match og efter overførsel af en beskrivelse af kendsgerningerne og en angivelse af den tilgrundliggende lovovertrædelse ved hjælp af den fælles tabel over strafbare handlinger, der er omhandlet i en gennemførelsesretsakt, der skal vedtages i henhold til rammeafgørelse 2009/315/RIA, bør den anmodende medlemsstat returnere et begrænset sæt af centrale data via routeren inden for 48 timer efter at de relevante betingelser er blevet opfyldt, medmindre der kræves en retskendelse i henhold til national ret.

(31) Data, der leveres og modtages på lovlig vis i henhold til denne forordning, er underlagt tidsfristerne for opbevaring og revision i medfør af direktiv (EU) 2016/680.

(32) Standarden for det universelle meddelelsesformat (UMF) bør anvendes ved udviklingen af routeren og EPRIS, så vidt den finder anvendelse. Enhver automatiseret udveksling af data i henhold til denne forordning bør anvende UMF-standarden, så vidt den finder anvendelse. Medlemsstaternes kompetente myndigheder og Europol opfordres også til at anvende UMF-standarden i forbindelse med enhver yderligere udveksling af data mellem dem for så vidt angår Prüm II-rammen. UMF-standarden bør være standarden for struktureret, grænseoverskridende informationsudveksling mellem informationssystemer, myndigheder eller organisationer på området for retlige og indre anliggender.

(33) Kun ikkeklassificerede information bør udveksles via Prüm II-rammen.

(34) Hver medlemsstat bør underrette de øvrige medlemsstater, Kommissionen, Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA), oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2018/1726[14], og Europol om indholdet af sin nationale databaser, der stilles til rådighed via Prüm II-rammen og om betingelserne for automatiserede søgninger.

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

(35) Visse aspekter af Prüm II-rammen kan ikke dækkes udtømmende af denne forordning på grund af deres tekniske, stærkt detaljerede og hyppigt skiftende karakter. Disse aspekter omfatter f.eks. tekniske ordninger og specifikationer for automatiserede søgeprocedurer, standarder for dataudveksling, herunder minimumskvalitetsstandarder, og de dataelementer, der skal udveksles. For at sikre ensartede betingelser for gennemførelsen af denne forordning for så vidt angår sådanne aspekter bør Kommissionen tillægges gennemførelsesbeføjelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011[15].

(36) Datakvalitet er af allerstørste betydning som en sikkerhedsforanstaltning og en væsentlig forudsætning for at sikre effektiviteten af denne forordning. I forbindelse med automatiserede søgninger efter biometriske data og for at sikre, at kvaliteten af de overførte data er tilstrækkelig høj, og reducere risikoen for falske match, bør der fastsættes en minimumskvalitetsstandard, som regelmæssigt bør revideres.

---

[15] 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).

(37) I betragtning af omfanget og følsomheden af de personoplysninger, der udveksles med henblik på denne forordning, og de forskellige nationale regler for lagring af oplysninger om enkeltpersoner i nationale databaser er det vigtigt at sikre, at de databaser, der anvendes til automatiseret søgning i henhold til denne forordning, er oprettet i overensstemmelse med national ret og direktiv (EU) 2016/680. Medlemsstaterne bør derfor, inden de forbinder deres nationale databaser med routeren eller EPRIS, foretage en konsekvensanalyse vedrørende databeskyttelse som omhandlet i direktiv (EU) 2016/680 og, hvor det er relevant, høre tilsynsmyndigheden som fastsat i nævnte direktiv.

(38) Medlemsstaterne og Europol bør sikre nøjagtigheden og relevansen af personoplysninger, der behandles i medfør af denne forordning. Hvor en medlemsstat eller Europol bliver opmærksom på, at der er blevet leveret data, som er ukorrekte eller ikke længere ajourførte eller ikke burde være leveret, bør dette uden unødigt ophold meddeles til den medlemsstat, der har modtaget dataene, eller til Europol, alt efter hvad der er relevant. Alle berørte medlemsstater eller Europol, alt efter hvad der er tilfældet, bør uden unødigt ophold berigtige eller slette dataene i overensstemmelse hermed. Hvor den medlemsstat, der modtog dataene, eller Europol har grund til at tro, at de leverede data er ukorrekte eller bør slettes, bør den eller det underrette den medlemsstat, der har leveret oplysningerne, uden unødigt ophold.

(39) Effektiv overvågning af gennemførelsen af denne forordning er af afgørende betydning. Navnlig bør overholdelsen af regler om behandling af personoplysninger være omfattet af effektive sikkerhedsforanstaltninger, og der bør sikres regelmæssig overvågning og revision, som foretages af dataansvarlige, tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse, alt efter hvad der er relevant. Bestemmelser, der giver mulighed for regelmæssig kontrol af antageligheden af forespørgsler databehandlingen lovlighed, bør også indføres.

(40) Tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse bør sikre koordineret tilsyn med anvendelsen af denne forordning inden for rammerne af deres ansvarsområder, navnlig hvis de identificerer væsentlige uoverensstemmelser mellem medlemsstaternes praksis eller potentielt ulovlige overførsler.

(41) Ved gennemførelsen af denne forordning er det afgørende, at medlemsstaterne og Europol noterer sig EU-Domstolens retspraksis vedrørende udvekslingen af biometriske data.

(42) Tre år efter idriftsættelsen af routeren og EPRIS og derefter hvert fjerde år bør Kommissionen udarbejde en evalueringsrapport, der omfatter en vurdering af medlemsstaternes og Europols anvendelse af denne forordning, navnlig deres overholdelse af de relevante databeskyttelsesforanstaltninger. Evalueringsrapporter bør også indeholde en vurdering af de opnåede resultater set i forhold til denne forordnings mål og dens indvirkning på de grundlæggende rettigheder. Evalueringsrapporter bør også evaluere Prüm II-rammens indvirkning, virksomhed, effektivitet, virkningsfuldhed, sikkerhed og arbejdsmetoder.

(43) Da denne forordning indeholder bestemmelser om etablering af en ny Prümramme, bør de bestemmelser i afgørelse 2008/615/RIA og 2008/616/RIA, der ikke længere er relevante, udgå. Nævnte afgørelser bør ændres i overensstemmelse hermed.

(44) Da routeren skal udvikles og forvaltes af eu-LISA, bør forordning (EU) 2018/1726 ændres ved at tilføje dette til eu-LISA's opgaver.

(45) Målene for denne forordning, nemlig at intensivere det grænseoverskridende politisamarbejde og give medlemsstaternes kompetente myndigheder mulighed for at søge efter forsvundne personer og identificere uidentificerede menneskelige rester, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang og virkninger bedre nås på EU-plan; Unionen kan vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union (TEU). I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå disse mål.

(46) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til TEU og til TEUF, deltager Danmark ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Danmark.

(47) I medfør af artikel 3 i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til TEU og til TEUF, har Irland meddelt, at det ønsker at deltage i vedtagelsen og anvendelsen af denne forordning.

(48) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725 og afgav en udtalelse den 2. marts 2022[16] —

VEDTAGET DENNE FORORDNING:

[16] EUT C 225 af 9.6.2022, s. 6.

Kapitel 1
Almindelige bestemmelser

Artikel 1

Genstand

Denne forordning fastlægger en ramme for søgning og udveksling af data mellem medlemsstaternes kompetente myndigheder (Prüm II-rammen) ved at fastsætte:

a) betingelserne og procedurerne for automatiseret søgning efter DNA-profiler, fingeraftryksdata, visse køretøjsregistreringsdata, ansigtsbilleder og politiregistre, og

b) reglerne for udveksling af centrale data efter et bekræftet match mellem biometriske data.

Artikel 2

Formål

Formålet med Prüm II-rammen er at intensivere det grænseoverskridende samarbejde i spørgsmål, der er omfattet af tredje del, afsnit V, kapitel 4 og 5, i traktaten om Den Europæiske Unions funktionsmåde, navnlig ved at lette udvekslingen af oplysninger mellem medlemsstaternes kompetente myndigheder, under fuld overholdelse af fysiske personers grundlæggende rettigheder, herunder retten til respekt for sit privatliv og retten til beskyttelse af personoplysninger, i overensstemmelse med Den Europæiske Unions charter om grundlæggende rettigheder.

Formålet med Prüm II-rammen er også at give medlemsstaternes kompetente myndigheder mulighed for at søge efter forsvundne personer i forbindelse med en strafferetlig efterforskning eller af humanitære årsager og at identificere menneskelige rester i overensstemmelse med artikel 29, forudsat at disse myndigheder har beføjelse til at foretage sådanne søgninger og foretage sådanne identifikationer i henhold til national ret.

Artikel 3

Anvendelsesområde

Denne forordning finder anvendelse på databaser, der er oprettet i overensstemmelse med national ret, og som anvendes til automatiseret overførsel af DNA-profiler, fingeraftryksdata, visse køretøjsregistreringsdata, ansigtsbilleder og politiregistre under overholdelse af direktiv (EU) 2016/680 eller forordning (EU) 2018/1725, (EU) 2016/794 eller (EU) 2016/679, alt efter hvad der er relevant.

Artikel 4

Definitioner

I denne forordning forstås ved:

1) "loci"(ental: "locus"): DNA-positioner, der indeholder identifikationskendetegn for en analyseret menneskelig DNA-prøve

2) "DNA-profil": en bogstav- eller nummerkode, der repræsenterer en række loci, eller den særlige molekylestruktur på de forskellige loci

3) "DNA-referencedata": DNA-profil og det referencenummer, der er omhandlet i artikel 7

4) "identificeret DNA-profil": en identificeret persons DNA-profil

5) "uidentificeret DNA-profil": en DNA-profil, der er indsamlet under efterforskningen af strafbare handlinger, og som stammer fra en endnu ikke identificeret person, herunder en DNA-profil opnået fra spor

6) "fingeraftryksdata": billeder af fingeraftryk, billeder af latente fingeraftryk, billeder af håndfladeaftryk, billeder af latente håndfladeaftryk og skabeloner af sådanne billeder (kodede minutiae), der er lagret og behandlet i en automatiseret database

7) "fingeraftryksreferencedata": fingeraftryksdata og det referencenummer, der er omhandlet i artikel 12

8) "uidentificerede fingeraftryksdata": fingeraftryksdata, der er indsamlet under efterforskningen af en strafbar handling, og som stammer fra en endnu ikke identificeret person, herunder fingeraftryksdata opnået fra spor

9) "identificerede fingeraftryksdata": en identificeret persons fingeraftryksdata

10) "individuel sag": et enkelt dossier, der vedrører forebyggelse, afsløring eller efterforskning af en strafbar handling, søgning efter en forsvundet person eller identifikation af uidentificerede menneskelige rester

11) "ansigtsbillede": et digitalt billede af ansigtet

12) "ansigtsbilledreferencedata": et ansigtsbillede og det referencenummer, der er omhandlet i artikel 21

13) "uidentificeret ansigtsbillede": et ansigtsbillede, der er indsamlet under efterforskningen af en strafbar handling, og som stammer fra en endnu ikke identificeret person, herunder et ansigtsbillede opnået fra spor

14) "identificeret ansigtsbillede": en identificeret persons ansigtsbillede

15) "biometriske data": DNA-profiler, fingeraftryksdata eller ansigtsbilleder

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

17) "match": eksistensen af et sammenfald som resultat af en automatiseret sammenligning mellem personoplysninger i en database

18) "kandidat": data, for hvilke der er et match

19) "anmodende medlemsstat": en medlemsstat, der foretager en søgning ved hjælp af Prüm II-rammen

20) " anmodede medlemsstat": en medlemsstat, i hvis databaser en anmodende medlemsstat foretager en søgning ved hjælp af Prüm II-rammen

21) "politiregistre": mistænktes og dømte personers biografiske data, der er tilgængelige i nationale databaser oprettet med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger

22) "pseudonymisering": pseudonymisering som defineret i artikel 3, nr. 5), i direktiv (EU) 2016/680

23) "mistænkt": en person som omhandlet i artikel 6, litra a), i direktiv (EU) 2016/680

24) "personoplysninger": personoplysninger som defineret i artikel 3, nr. 1), i direktiv (EU) 2016/680

25) "Europoldata": operationelle personoplysninger, der behandles af Europol i overensstemmelse med forordning (EU) 2016/794

26) "kompetent myndighed": enhver offentlig myndighed, der er kompetent med hensyn til at forebygge, afsløre eller efterforske strafbare handlinger, eller ethvert andet organ eller enhver anden enhed, som i henhold til medlemsstaternes nationale ret udøver offentlig myndighed og offentlige beføjelser med henblik på at forebygge, afsløre eller efterforske strafbare handlinger

27) "tilsynsmyndighed": en uafhængig offentlig myndighed, der er oprettet af en medlemsstat i medfør af artikel 41 i direktiv (EU) 2016/680

28) "SIENA": en sikker netværksapplikation til udveksling af oplysninger, der forvaltes og udvikles af Europol i overensstemmelse med forordning (EU) 2016/794

29) "hændelse": en hændelse som defineret i artikel 6, nr. 6), i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[17]

30) "væsentlig hændelse": en hændelse, medmindre denne hændelse har en begrænset indvirkning og sandsynligvis allerede er velforstået med hensyn til metode eller teknologi

31) "væsentlig cybertrussel": en cybertrussel, der har mulighed og evne til, og hvis formål er, at forårsage en væsentlig hændelse

32) "væsentlig sårbarhed": en sårbarhed, der sandsynligvis vil føre til en væsentlig hændelse, hvis den udnyttes.

[17] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

Kapitel 2
Udveksling af data

AFSNIT 1
DNA-PROFILER

Artikel 5
DNA-referencedata

1. Medlemsstaterne sikrer tilgængeligheden af DNA-referencedata fra deres nationale DNA-databaser med henblik på andre medlemsstaters og Europols automatiserede søgning i medfør af denne forordning.

   DNA-referencedata må ikke indeholde yderligere data, som gør det muligt at identificere en person direkte.

   Uidentificerede DNA-profiler skal være genkendelige som sådanne.

2. DNA-referencedata behandles i overensstemmelse med denne forordning og under overholdelse af den nationale ret, der finder anvendelse på behandlingen af disse data.

3. Kommissionen vedtager en gennemførelsesretsakt med henblik på at præcisere de identifikationskendetegn for en DNA-profil, der skal udveksles. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 6

Automatiseret søgning efter DNA-profiler

1. Med henblik på efterforskning af strafbare handlinger foretager medlemsstaterne, på det tidspunkt de første gang etablerer forbindelse til routeren via deres nationale kontaktpunkter, en automatiseret søgning ved at sammenligne alle DNA-profilerne lagret i deres nationale DNA-databaser med alle DNA-profilerne lagret i alle andre medlemsstaters DNA-databaser og i Europoldata. Hver medlemsstat aftaler bilateralt med hver anden medlemsstat og med Europol ordningerne for disse automatiserede søgninger i overensstemmelse med de regler og procedurer, der er fastsat i denne forordning.

2. Med henblik på efterforskning af strafbare handlinger foretager medlemsstaterne via deres nationale kontaktpunkter automatiserede søgninger ved at sammenligne alle de nye DNA-profiler, der er tilføjet til deres DNA-database, med alle DNA-profilerne lagret i alle andre medlemsstaters DNA-databaser og i Europoldata.

3. Hvis søgninger som omhandlet i stk. 2 ikke kan finde sted, kan den berørte medlemsstat bilateralt aftale med hver anden medlemsstat og med Europol at foretage dem på et senere tidspunkt ved at sammenligne DNA-profiler med alle DNA-profiler lagret i alle andre medlemsstaters DNA-databaser og i Europoldata. Den berørte medlemsstat aftaler bilateralt med hver anden medlemsstat og med Europol ordningerne for disse automatiserede søgninger i overensstemmelse med de regler og procedurer, der er fastsat i denne forordning.

4. Søgninger som omhandlet i stk. 1, 2 og 3 må kun foretages i forbindelse med individuelle sager og under overholdelse af den anmodende medlemsstats nationale ret.

5. Hvis det ved en automatiseret søgning konstateres, at en leveret DNA-profil matcher en DNA-profil, der er lagret i den anmodede medlemsstats database eller databaser, modtager den anmodende medlemsstats nationale kontaktpunkt på en automatiseret måde de DNA-referencedata, som der er konstateret et match med.

6. Den anmodende medlemsstats nationale kontaktpunkt kan beslutte at bekræfte et match mellem to DNA-profiler. Hvor det beslutter at bekræfte en match mellem to DNA-profiler, underretter det den anmodede medlemsstat og sikrer, at mindst én kvalificeret medarbejder foretager en manuel gennemgang for at bekræfte dette match med de DNA-referencedata, der er modtaget fra den anmodede medlemsstat.

7. Hvor det er relevant for efterforskningen af strafbare handlinger kan den anmodede medlemsstats nationale kontaktpunkt også beslutte at bekræfte et match mellem to DNA-profiler. Hvor det beslutter at bekræfte en match mellem to DNA-profiler, underretter det den anmodende medlemsstat og sikrer, at mindst én kvalificeret medarbejder foretager en manuel gennemgang for at bekræfte dette match med de DNA-referencedata, der er modtaget fra den anmodende medlemsstat.

Artikel 7

Referencenumre for DNA-profiler

Referencenumrene for DNA-profiler er en kombination af følgende:

a) et referencenummer, der i tilfælde af et match gør det muligt for medlemsstaterne at hente yderligere data og andre oplysninger i deres nationale databaser med henblik på at levere dem til en, flere eller alle andre medlemsstater i overensstemmelse med artikel 47 eller til Europol i overensstemmelse med artikel 49, stk. 6

b) et referencenummer, der i tilfælde af et match gør det muligt for Europol at hente yderligere data og andre oplysninger med henblik på denne forordnings artikel 48, stk. 1, for at levere dem til en, flere eller alle medlemsstater i overensstemmelse med forordning (EU) 2016/794

c) en kode til angivelse af den medlemsstat, der ligger inde med DNA-profilen

d) en kode til angivelse af, hvorvidt DNA-profilen er en identificeret DNA-profil eller en uidentificeret DNA-profil.

Artikel 8

Principper for udveksling af DNA-profiler

1. Medlemsstaterne træffer passende foranstaltninger for at sikre fortroligheden og integriteten af DNA-referencedata, der sendes til andre medlemsstater eller Europol, herunder kryptering heraf. Europol træffer passende foranstaltninger for at sikre fortroligheden og integriteten af DNA-referencedata, der sendes til medlemsstater, herunder kryptering heraf.

2. Hver medlemsstat og Europol sikrer, at kvaliteten af de DNA-profiler, som overføres, er tilstrækkelig høj til automatiseret sammenligning. Kommissionen fastsætter ved hjælp af gennemførelsesretsakter en minimumskvalitetsstandard for at muliggøre sammenligningen af DNA-profiler.

3. Kommissionen vedtager gennemførelsesretsakter, der angiver de relevante europæiske eller internationale standarder, der skal anvendes af medlemsstaterne og Europol til udveksling af DNA-referencedata.

4. De i denne artikels stk. 2 og 3 omhandlede gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 9

Regler for anmodninger og svar vedrørende DNA-profiler

1. En anmodning om automatiseret søgning af DNA-profiler må kun indeholde følgende oplysninger:

   a) den anmodende medlemsstats kode

   b) dato og tidspunkt for anmodningen samt anmodningsnummer

   c) DNA-referencedata

   d) hvorvidt de fremsendte DNA-profiler er uidentificerede DNA-profiler eller identificerede DNA-profiler.

2. Et svar på en anmodningen som omhandlet i stk. 1 må kun indeholde følgende oplysninger:

   a) en angivelse af, hvorvidt der er konstateret et eller flere match eller ej

   b) dato og tidspunkt for anmodningen samt anmodningsnummer

   c) dato og tidspunkt for svaret samt svarnummer

   d) koderne for den anmodende og den anmodede medlemsstat

e) referencenumrene på DNA-profilerne fra den anmodende og den anmodede medlemsstat

f) hvorvidt de fremsendte DNA-profiler er uidentificerede DNA-profiler eller identificerede DNA-profiler

g) de matchende DNA-profiler.

3. Der gives kun automatisk meddelelse om et match, hvis den automatiserede søgning har resulteret i et match mellem et mindste antal loci. Kommissionen vedtager gennemførelsesretsakter, der angiver det mindste antal loci for dette formål, efter undersøgelsesproceduren i artikel 77, stk. 2.

4. Hvis en søgning med uidentificerede DNA-profiler resulterer i et match, kan hver anmodet medlemsstat med matchende data indsætte en mærkning i sin nationale database, der angiver, at der har været et match for den pågældende DNA-profil efter en anden medlemsstats søgning. Denne mærkning skal indeholde referencenummeret for den DNA-profil, der blev anvendt af den anmodende medlemsstat.

5. Medlemsstaterne sikrer, at anmodninger som omhandlet i denne artikels stk. 1 stemmer overens med de meddelelser, der sendes i henhold til artikel 74. Disse meddelelser gengives i den praktiske håndbog, der er omhandlet i artikel 79.

AFSNIT 2

FINGERAFTRYKSDATA

Artikel 10

Fingeraftryksreferencedata

1. Medlemsstaterne sikrer tilgængeligheden af fingeraftryksreferencedata fra deres nationale databaser oprettet med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger.

2. Fingeraftryksreferencedata må ikke indeholde yderligere data, som gør det muligt at identificere en fysisk person direkte.

3. Uidentificerede fingeraftryksdata skal være genkendelige som sådanne.

Artikel 11

Automatiseret søgning efter fingeraftryksdata

1. Med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger giver medlemsstaterne andre medlemsstaters nationale kontaktpunkter og Europol adgang til fingeraftryksreferencedataene i deres nationale databaser oprettet til dette formål for at foretage automatiseret søgning ved at sammenligne fingeraftryksreferencedata.

Søgninger som omhandlet i første afsnit må kun foretages i forbindelse med individuelle sager og under overholdelse af den anmodende medlemsstats nationale ret.

2. Den anmodende medlemsstats nationale kontaktpunkt kan beslutte at bekræfte et match mellem to sæt fingeraftryksdata. Hvis det beslutter at bekræfte et match mellem to sæt fingeraftryksdata, underretter det den anmodede medlemsstat og sikrer, at mindst én kvalificeret medarbejder foretager en manuel gennemgang for at bekræfte dette match med de fingeraftryksreferencedata, der er modtaget fra den anmodede medlemsstat.

Artikel 12

Referencenumre for fingeraftryksdata

Referencenumrene for fingeraftryksdata er en kombination af følgende:

a) et referencenummer, der i tilfælde af et match gør det muligt for medlemsstater at hente yderligere data og andre oplysninger i deres i artikel 10 omhandlede databaser med henblik på at levere dem til en, flere eller alle andre medlemsstater i overensstemmelse med artikel 47 eller til Europol i overensstemmelse med artikel 49, stk. 6

b) et referencenummer, der i tilfælde af et match gør det muligt for Europol at hente yderligere data og andre oplysninger med henblik på denne forordnings artikel 48, stk. 1, for at levere dem til en, flere eller alle medlemsstater i overensstemmelse med forordning (EU) 2016/794

c) en kode til angivelse af den medlemsstat, der ligger inde med fingeraftryksdataene.

Artikel 13

Principper for udveksling af fingeraftryksdata

1. Medlemsstaterne træffer passende foranstaltninger til at sikre fortroligheden og integriteten af fingeraftryksdata, der sendes til andre medlemsstater eller Europol, herunder kryptering heraf. Europol træffer passende foranstaltninger til at sikre fortroligheden og integriteten af fingeraftryksdata, der sendes til medlemsstater, herunder kryptering heraf.

2. Hver medlemsstat og Europol sikrer, at kvaliteten af de fingeraftryksdata, som overføres, er tilstrækkelig høj til automatiseret sammenligning. Kommissionen fastsætter ved hjælp af gennemførelsesretsakter en minimumskvalitetsstandard for at muliggøre sammenligningen af fingeraftryksdata.

3. Fingeraftryksdata digitaliseres og overføres til de øvrige medlemsstater eller Europol i overensstemmelse med europæiske eller internationale standarder. Kommissionen vedtager gennemførelsesretsakter, der angiver de relevante europæiske eller internationale standarder, der skal anvendes af medlemsstaterne og Europol til udveksling af fingeraftryksdata.

4. De i denne artikels stk. 2 og 3 omhandlede gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 14

Søgekapacitet for fingeraftryksdata

1. Hver medlemsstat sikrer, at dets søgningsanmodninger ikke overstiger den søgekapacitet, som den anmodede medlemsstat eller Europol har anført, for at sikre systemets parathed og undgå, at systemet overbelastes. Med det samme formål sikrer Europol, at dets søgningsanmodninger ikke overstiger den søgekapacitet, som den anmodede medlemsstat har anført.

   Medlemsstaterne underretter de øvrige medlemsstater, Kommissionen, eu-LISA og Europol om deres maksimale søgekapacitet pr. dag for identificerede og uidentificerede fingeraftryksdata. Europol underretter medlemsstaterne, Kommissionen og eu-LISA om dets maksimale søgekapacitet pr. dag for identificerede og uidentificerede fingeraftryksdata. Medlemsstaterne eller Europol kan til enhver tid, herunder i hastetilfælde, øge denne søgekapacitet midlertidigt eller permanent. Hvor en medlemsstat forhøjer denne maksimale søgekapacitet, underretter den de øvrige medlemsstater, Kommissionen, eu-LISA og Europol om den nye maksimale søgekapacitet. Hvor Europol forhøjer denne maksimale søgekapacitet, underretter det medlemsstaterne, Kommissionen og eu-LISA om den nye maksimale søgekapacitet.

2. Kommissionen vedtager gennemførelsesretsakter, der angiver det maksimale antal kandidater, der accepteres til sammenligning pr. fremsendelse, og fordelingen af uudnyttet søgekapacitet mellem medlemsstaterne, efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 15

Regler for anmodninger og svar vedrørende fingeraftryksdata

1. En anmodning om automatiseret søgning af fingeraftryksdata må kun indeholde følgende oplysninger:

   a) den anmodende medlemsstats kode

   b) dato og tidspunkt for anmodningen samt anmodningsnummer

   c) fingeraftryksreferencedataene.

2. Et svar på en anmodning som omhandlet i stk. 1 må kun indeholde følgende oplysninger:

   a) en angivelse af, hvorvidt der er konstateret et eller flere match eller ej

   b) dato og tidspunkt for anmodningen samt anmodningsnummer

   c) dato og tidspunkt for svaret samt svarnummer

d) koderne for den anmodende og den anmodede medlemsstat

e) referencenumrene på fingeraftryksdataene fra de anmodende og anmodede medlemsstater

f) de matchende fingeraftryksdata.

3. Medlemsstaterne sikrer, at anmodninger som omhandlet i denne artikels stk. 1 stemmer overens med de meddelelser, der sendes i henhold til artikel 74. Disse meddelelser gengives i den praktiske håndbog, der er omhandlet i artikel 79.

AFSNIT 3

KØRETØJSREGISTRERINGSDATA

Artikel 16

Automatiseret søgning efter køretøjsregistreringsdata

1. Med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger giver medlemsstaterne andre medlemsstaters nationale kontaktpunkter og Europol adgang til følgende nationale køretøjsregistreringsdata med henblik på at foretage automatiseret søgning i individuelle sager:

a) data vedrørende ejeren eller indehaveren af køretøjet

b) data vedrørende køretøjet.

2. Søgninger som omhandlet i stk. 1 må kun foretages med følgende date:

a) et fuldstændigt chassisnummer

b) et fuldstændigt registreringsnummer, eller

c) hvor dette er tilladt i henhold til den anmodede medlemsstats national ret, data vedrørende ejeren eller indehaveren af køretøjet.

3. Søgninger som omhandlet i stk. 1 foretaget på grundlag af data vedrørende ejeren eller indehaveren af køretøjet må kun foretages for så vidt angår mistænkte eller dømte personer. Alle følgende identifikationsdata anvendes med henblik på sådanne søgninger:

a) hvor ejeren eller indehaveren af køretøjet er en fysisk person:

i) den fysiske persons fornavn eller fornavne

ii) den fysiske persons efternavn eller efternavne, og

iii) den fysiske persons fødselsdato

b) hvor ejeren eller indehaveren af køretøjet er en juridisk person, denne juridiske persons navn.

4. Søgninger som omhandlet i stk. 1 må kun foretages under overholdelse af den anmodende medlemsstats nationale ret.

Artikel 17

Principper for elektronisk søgning efter køretøjsregistreringsdata

1. Til automatiseret søgning efter køretøjsregistreringsdata anvender medlemsstaterne det europæiske informationssystem vedrørende køretøjer og kørekort (Eucaris).

2. Oplysninger, der udveksles via Eucaris, overføres i krypteret form.

3. Kommissionen vedtager gennemførelsesretsakter, der angiver dataelementerne i de køretøjsregistreringsdata, der kan udveksles, og den tekniske procedure for Eucaris til at foretage forespørgsler i medlemsstaternes databaser. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 18

Føring af logfiler

1. Hver medlemsstat fører logfiler over forespørgsler, som dens kompetente myndigheds personale, der er behørigt bemyndiget til at udveksle køretøjsregistreringsdata, foretager, samt logfiler over forespørgsler, som andre medlemsstater har anmodet om. Europol fører logfiler over forespørgsler, som dets behørigt bemyndigede personale foretager.

Hver medlemsstat og Europol fører logfiler over alle databehandlingsaktiviteter vedrørende køretøjsregistreringsdata. Disse logfiler omfatter følgende:

a) hvorvidt det var en medlemsstat eller Europol, der fremsatte anmodningen om en forespørgsel; såfremt det var en medlemsstat, der fremsatte anmodningen om en forespørgsel, den pågældende medlemsstat

b) dato og klokkeslæt for forespørgslen

c) dato og klokkeslæt for svaret

d) de nationale databaser, hvortil en anmodning om en forespørgsel blev sendt

e) de nationale databaser, der gav et positivt svar.

2. De i stk. 1 omhandlede logfiler må kun anvendes til indsamling af statistikker, til overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, og til sikring af datasikkerhed og -integritet. Disse logfiler beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes tre år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige for overvågningsprocedurerne.

3. Med henblik på overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, har de dataansvarlige adgang til logfilerne til egenkontrol som omhandlet i artikel 55.

AFSNIT 4

ANSIGTSBILLEDER

Artikel 19

Ansigtsbilledereferencedata

1. Medlemsstaterne sikrer tilgængeligheden af ansigtsbilledereferencedata vedrørende mistænkte, dømte personer og, hvor det er tilladt i henhold til national ret, ofre fra deres nationale databaser oprettet med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger.

2. Ansigtsbilledereferencedata må ikke indeholde yderligere data, som gør det muligt at identificere en fysisk person direkte.

3. Uidentificerede ansigtsbilleder skal være genkendelige som sådanne.

Artikel 20

Automatiseret søgning efter ansigtsbilleder

1. Med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger, der kan straffes med en maksimal fængselsstraf på mindst ét år henhold til den anmodende medlemsstats nationale ret, giver medlemsstaterne andre medlemsstaters nationale kontaktpunkter og Europol adgang til ansigtsbilledereferencedataene i deres nationale databaser med henblik på at foretage automatiserede søgninger.

   Søgninger som omhandlet i første afsnit må kun foretages i forbindelse med individuelle sager og under overholdelse af den anmodende medlemsstats nationale ret.

   Profilering som omhandlet i artikel 11, stk. 3, i direktiv (EU) 2016/680 er forbudt.

2. Den anmodende medlemsstats nationale kontaktpunkt kan beslutte at bekræfte et match mellem to ansigtsbilleder. Hvis det beslutter at bekræfte et match mellem to ansigtsbilleder, underretter det den anmodede medlemsstat og sikrer, at mindst én kvalificeret medarbejder foretager en manuel gennemgang for at bekræfte dette match med de ansigtsbilledereferencedata, der er modtaget fra den anmodede medlemsstat.

Artikel 21

Referencenumre for ansigtsbilleder

Referencenumrene for ansigtsbilleder er en kombination af følgende:

a) et referencenummer, der i tilfælde af et match gør det muligt for medlemsstater at hente yderligere data og andre oplysninger i deres i artikel 19 omhandlede databaser med henblik på at levere dem til en, flere eller alle andre medlemsstater i overensstemmelse med artikel 47 eller til Europol i overensstemmelse med artikel 49, stk. 6

b) et referencenummer, der i tilfælde af et match gør det muligt for Europol at hente yderligere data og andre oplysninger med henblik på denne forordnings artikel 48, stk. 1, for at levere dem til en, flere eller alle andre medlemsstater i overensstemmelse med forordning (EU) 2016/794

c) en kode til angivelse af den medlemsstat, der ligger inde med ansigtsbillederne.

Artikel 22

Principper for udveksling af ansigtsbilleder

1. Medlemsstaterne træffer passende foranstaltninger til at sikre fortroligheden og integriteten af ansigtsbilleder, der sendes til andre medlemsstater eller Europol, herunder kryptering heraf. Europol træffer passende foranstaltninger til at sikre fortroligheden og integriteten af ansigtsbilleder, der sendes til medlemsstater, herunder kryptering heraf.

2. Hver medlemsstat og Europol sikrer, at kvaliteten af de ansigtsbilleder, som overføres, er tilstrækkelig høj til automatiseret sammenligning. Kommissionen fastsætter ved hjælp af gennemførelsesretsakter en minimumskvalitetsstandard for at muliggøre sammenligningen af ansigtsbilleder. Hvis den rapport, der er omhandlet i artikel 80, stk. 7, viser, at der er en høj risiko for falske match, reviderer Kommissionen disse gennemførelsesretsakter.

3. Kommissionen vedtager gennemførelsesretsakter, der angiver de relevante europæiske eller internationale standarder, der skal anvendes af medlemsstaterne og Europol til udveksling af ansigtsbilleder.

4. De i denne artikels stk. 2 og 3 omhandlede gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 23

Søgekapacitet for ansigtsbilleder

1. Hver medlemsstat sikrer, at dets søgningsanmodninger ikke overstiger den søgekapacitet, som den anmodede medlemsstat eller Europol har anført, for at sikre systemets parathed og undgå, at systemet overbelastes. Med det samme formål sikrer Europol, at dets søgningsanmodninger ikke overstiger den søgekapacitet, som den anmodede medlemsstat har anført.

Medlemsstaterne underretter de øvrige medlemsstater, Kommissionen, eu-LISA og Europol om deres maksimale søgekapacitet pr. dag for identificerede og uidentificerede ansigtsbilleder. Europol underretter medlemsstaterne, Kommissionen og eu-LISA om dets maksimale søgekapacitet pr. dag for identificerede og uidentificerede ansigtsbilleder. Medlemsstaterne eller Europol kan til enhver tid, herunder i hastetilfælde, øge denne søgekapacitet midlertidigt eller permanent. Hvor en medlemsstat forhøjer denne maksimale søgekapacitet, underretter den de andre medlemsstater Kommissionen, eu-LISA og Europol om den nye maksimale søgekapacitet. Hvor Europol forhøjer denne maksimale søgekapacitet, underretter det medlemsstaterne, Kommissionen og eu-LISA om den nye maksimale søgekapacitet.

2. Kommissionen vedtager gennemførelsesretsakter, der angiver det maksimale antal kandidater, der accepteres til sammenligning pr. fremsendelse, og fordelingen af uudnyttet søgekapacitet mellem medlemsstaterne, efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 24

Regler for anmodninger og svar vedrørende ansigtsbilleder

1. En anmodning om automatiseret søgning af ansigtsbilleder må kun indeholde følgende oplysninger:

   a) den anmodende medlemsstats kode

b) dato og tidspunkt for anmodningen samt anmodningsnummer

c) ansigtsbilledereferencedata.

2. Et svar på en anmodning som omhandlet i stk. 1 må kun indeholde følgende oplysninger:

a) en angivelse af, hvorvidt der er konstateret et eller flere match eller ej

b) dato og tidspunkt for anmodningen samt anmodningsnummer

c) dato og tidspunkt for svaret samt svarnummer

d) koderne for den anmodende og den anmodede medlemsstat

e) referencenumrene på ansigtsbillederne fra den anmodende og den anmodede medlemsstat

f) de matchende ansigtsbilleder.

3. Medlemsstaterne sikrer, at anmodninger som omhandlet i denne artikels stk. 1 stemmer overens med de meddelelser, der sendes i henhold til artikel 74. Disse meddelelser gengives i den praktiske håndbog, der er omhandlet i artikel 79.

AFSNIT 5

POLITIREGISTRE

Artikel 25

Politiregistre

1. Medlemsstaterne kan deltage i den automatiserede udveksling af politiregistre. Med henblik på sådanne udvekslinger sikrer deltagende medlemsstater tilgængeligheden af nationale politiregisterindekser, som indeholder mistænktes og dømte personers biografiske data, fra deres nationale databaser oprettet med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger. Disse datasæt skal alene indeholde følgende data, i det omfang de foreligger:

   a) fornavn eller fornavne

   b) efternavn eller efternavne

   c) kaldenavn eller kaldenavne og tidligere anvendt navn eller tidligere anvendte navne

   d) fødselsdato

   e) nationalitet eller nationaliteter

   f) fødeland

   g) køn.

2. De data, der er omhandlet i stk. 1, litra a), b) og c), skal være pseudonymiserede.

Artikel 26

Automatiseret søgning i nationale politiregisterindekser

Med henblik på forebyggelse, afsløring og efterforskning af strafbare handlinger, der kan straffes med en maksimal fængselsstraf på mindst ét år i henhold til den anmodende medlemsstats nationale ret, giver de medlemsstater, der deltager i den automatiserede udveksling af politiregistre, andre deltagende medlemsstaters nationale kontaktpunkter og Europol adgang til data fra deres nationale politiregisterindekser med henblik på at foretage automatiserede søgninger.

Søgninger som omhandlet i første afsnit må kun foretages i forbindelse med individuelle sager og under overholdelse af den anmodende medlemsstats nationale ret.

Artikel 27

Referencenumre for politiregistre

Referencenumrene for politiregistre er en kombination af følgende:

a) et referencenummer, der i tilfælde af match gør det muligt for medlemsstaterne at hente biografiske data og andre oplysninger i deres i artikel 25 omhandlede nationale politiregisterindekser med henblik på at levere dem til en, flere eller alle medlemsstater i overensstemmelse med artikel 44

b) en kode til angivelse af den medlemsstat, der ligger inde med politiregistrene.

Artikel 28

Regler for anmodninger og svar vedrørende politiregistre

1. En anmodning om automatiseret søgning i nationale politiregisterindekser må kun indeholde følgende oplysninger:

   a) den anmodende medlemsstats kode

   b) dato og tidspunkt for anmodningen samt anmodningsnummer

   c) dataene omhandlet i artikel 25, for så vidt som de foreligger.

2. Et svar på en anmodning som omhandlet i stk. 1 må kun indeholde følgende oplysninger:

   a) en angivelse af antallet af match

   b) dato og tidspunkt for anmodningen samt anmodningsnummer

   c) dato og tidspunkt for svaret samt svarnummer

   d) koderne for den anmodende og den anmodede medlemsstat

   e) referencenumrene for politiregistrene fra de anmodede medlemsstater.

3. Medlemsstaterne sikrer, at anmodninger som omhandlet i denne artikels stk. 1 stemmer overens med de meddelelser, der sendes i henhold til artikel 74. Disse meddelelser gengives i den praktiske håndbog, der er omhandlet i artikel 79.

AFSNIT 6

FÆLLES BESTEMMELSER

Artikel 29

Forsvundne personer og uidentificerede menneskelige rester

1. Hvor en national myndighed har beføjelse hertil i medfør af nationale lovgivningsmæssige foranstaltninger som omhandlet i stk. 2, må den foretage automatiserede søgninger ved anvendelse af Prüm II-rammen alene med henblik på:

   a) at søge efter forsvundne personer i forbindelse med strafferetlig efterforskning eller af humanitære årsager

   b) at identificere menneskelige rester.

2. Medlemsstater, der ønsker at benytte sig af den mulighed, som er fastsat i stk. 1, udpeger ved hjælp af nationale lovgivningsmæssige foranstaltninger de nationale myndigheder, der har kompetence til de deri angivne formål, og fastsætter procedurer, betingelser og kriterier, herunder de humanitære årsager på grundlag af hvilke det er tilladt at foretage automatiserede søgninger efter forsvundne personer som omhandlet i stk. 1, litra a).

Artikel 30

Nationale kontaktpunkter

Hver medlemsstat udpeger et eller flere nationale kontaktpunkter med henblik på artikel 6, 11, 16, 20 og 26.

Artikel 31

Gennemførelsesforanstaltninger

Kommissionen vedtager gennemførelsesretsakter, der angiver de tekniske ordninger, som medlemsstaterne skal træffe med hensyn til procedurerne i artikel 6, 11, 16, 20 og 26. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 32

Adgang til automatiseret udveksling af data på nationalt plan

1. Medlemsstaterne træffer alle nødvendige foranstaltninger for at sikre, at automatiseret søgning af DNA-profiler, fingeraftryksdata, køretøjsregistreringsdata, ansigtsbilleder og politiregistre er mulig døgnet rundt 7 dage om ugen.

2. De nationale kontaktpunkter underretter omgående hinanden, Kommissionen, eu-LISA og Europol i ethvert tilfælde, hvor den automatiserede dataudveksling ikke er tilgængelig, herunder i givet fald om alle tekniske fejl, der er årsag til denne utilgængelighed.

De nationale kontaktpunkter aftaler midlertidige alternative ordninger for udveksling af oplysninger i overensstemmelse med den gældende EU-ret og national ret, der skal anvendes, hvor den automatiseret udveksling af data ikke er tilgængelig.

3. Hvor den automatiserede udveksling af data er utilgængelig, sørger de nationale kontaktpunkter for, at den med alle nødvendige midler og straks genetableres.

Artikel 33

Begrundelse for behandling af data

1. Hver medlemsstat opbevarer en fortegnelse over begrundelserne for de forespørgsler, som dens kompetente myndigheder foretager.

Europol opbevarer en fortegnelse over begrundelserne for de forespørgsler, det foretager.

2. De i stk. 1 omhandlede begrundelser skal omfatte:

a) formålet med forespørgslen, herunder en henvisning til den specifikke sag eller undersøgelse og i givet fald til den strafbare handling

b) en angivelse af, hvorvidt forespørgslen vedrører en mistænkt eller en person, der er dømt for en strafbar handling, et offer for en strafbar handling, en forsvundet person eller uidentificerede menneskelige rester

c) en angivelse af, hvorvidt forespørgslen har til formål at identificere en person eller få flere data om en kendt person.

3. De i denne artikels stk. 1 omhandlede begrundelser skal kunne spores tilbage til logfilerne omhandlet i artikel 18, 40 og 45. Disse begrundelser må kun bruges til at vurdere, hvorvidt søgningerne er forholdsmæssige og nødvendige med henblik på at forebygge, afsløre eller efterforske en strafbar handling, og til overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, og til sikring af datasikkerhed og -integritet. Disse begrundelser beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes tre år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige for overvågningsprocedurerne.

4. Med henblik på vurdering af, om søgninger med det formål at forebygge, afsløre eller efterforske en strafbar handling er forholdsmæssige og nødvendige, og med henblik på overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, har de dataansvarlige adgang til disse begrundelser til egenkontrol som omhandlet i artikel 55.

Artikel 34

Anvendelse af det universelle meddelelsesformat

1. For så vidt som det er muligt, anvendes den standard for det universelle meddelelsesformat (UMF-standarden), som er oprettet ved artikel 38 i forordning (EU) 2019/818, ved udviklingen af router omhandlet i nærværende forordnings artikel 35 og det europæiske politiregisterindekssystem (EPRIS).

2. Enhver automatiseret udveksling af data i overensstemmelse med denne forordning skal anvende UMF-standarden, for så vidt som det er muligt.

Kapitel 3
Arkitektur

AFSNIT 1
ROUTER

Artikel 35
Router

1. Der oprettes en router med det formål at lette etableringen af forbindelser mellem medlemsstaterne og mellem medlemsstaterne og Europol, med henblik på at foretage forespørgsler i, hente og score biometriske data og med henblik på at hente alfanumeriske data i overensstemmelse med denne forordning.

2. Routeren skal bestå af:

   a) en central infrastruktur, herunder et søgeværktøj, der muliggør samtidige forespørgsler i de nationale databaser omhandlet i artikel 5, 10 og 19 og i Europoldata

   b) en sikker kommunikationskanal mellem den centrale infrastruktur, kompetente myndigheder, der er bemyndiget til at anvende routeren i medfør af artikel 36, og Europol

c) en sikker kommunikationsinfrastruktur mellem den centrale infrastruktur og den europæiske søgeportal, der er oprettet ved artikel 6 i forordning (EU) 2019/817 og artikel 6 i forordning (EU) 2019/818, med henblik på artikel 39.

Artikel 36

Anvendelse af routeren

Anvendelsen af routeren er forbeholdt de kompetente myndigheder i medlemsstaterne, der er bemyndiget til at få adgang til og udveksle DNA-profiler, fingeraftryksdata og ansigtsbilleder i overensstemmelse med denne forordning, og Europol i overensstemmelse med denne forordning og forordning (EU) 2016/794.

Artikel 37

Processer

1. De kompetente myndigheder, der er bemyndiget til at anvende routeren i medfør af artikel 36, eller Europol, anmoder om en forespørgsel ved at indsende biometriske data til routeren. Routeren sender anmodningen om en forespørgsel til alle eller specifikke medlemsstaters databaser og til Europoldata samtidig med de data, som brugeren har indsendt i overensstemmelse med vedkommendes adgangsrettigheder.

2. Ved modtagelse af en anmodning om en forespørgsel fra routeren, iværksætter hver anmodet medlemsstat straks en forespørgsel i deres databaser på en automatiseret måde. Ved modtagelse af en anmodning om en forespørgsel fra routeren, iværksætter Europol straks en forespørgsel i Europoldata på en automatiseret måde.

3. Eventuelle match, der opstår som følge af forespørgsler som omhandlet i stk. 2, sendes tilbage til routeren på en automatiseret måde. Den anmodende medlemsstat underrettes på en automatiseret måde, hvis der ikke er noget match.

4. Hvor den anmodende medlemsstat beslutter dette, og hvor det er relevant, rangordner routeren svarene ved at sammenligne de biometriske data anvendt til forespørgslerne og de biometriske data givet i svarene fra den anmodede medlemsstat eller de anmodede medlemsstater eller Europol.

5. Routeren returnerer listen over matchende biometriske data og deres rangorden til routerbrugeren.

6. Kommissionen vedtager gennemførelsesretsakter, der angiver den tekniske procedure for routerens forespørgsler i medlemsstaternes databaser og i Europoldataene, formatet for routerens svar på sådanne forespørgsler og de tekniske regler for sammenligning og rangordning af sammenfaldet mellem biometriske data. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 38

Kvalitetskontrol

Den anmodede medlemsstat kontrollerer kvaliteten af de fremsendte data ved hjælp af en automatiseret procedure.

Den anmodede medlemsstat underretter straks den anmodende medlemsstat via routeren, hvor dataene er uegnede til automatiseret sammenligning.

Artikel 39

Interoperabilitet mellem routeren og det fælles identitetsregister med henblik på adgang til retshåndhævelse

1. Hvor udpegede myndigheder som defineret i artikel 4, nr. 20), i forordning (EU) 2019/817 og artikel 4, nr. 20), i forordning (EU) 2019/818, er bemyndiget til at anvende routeren i medfør af denne forordnings artikel 36, kan de iværksætte en forespørgsel i medlemsstaternes databaser og i Europoldata samtidig med en forespørgsel til det fælles identitetsregister, der er oprettet ved artikel 17 i forordning (EU) 2019/817 og artikel 17 i forordning (EU) 2019/818, forudsat at de relevante betingelser i henhold til EU-retten er blevet opfyldt, og at forespørgslen er iværksat i overensstemmelse med deres adgangsrettigheder. Til dette formål søger routeren i det fælles identitetsregister via den europæiske søgeportal.

2. Forespørgsler til det fælles identitetsregister med henblik på retshåndhævelse foretages i overensstemmelse med artikel 22 i forordning (EU) 2019/817 og artikel 22 i forordning (EU) 2019/818. Ethvert resultat af sådanne forespørgsler sendes via den europæiske søgeportal.

Samtidige søgninger i medlemsstaternes databaser og i Europoldata og i det fælles identitetsregister må kun iværksættes i tilfælde, hvor der er rimelig grund til at antage, at data om en mistænkt, en gerningsmand eller et offer for en terrorhandling eller andre alvorlige strafbare handlinger som defineret i henholdsvis artikel 4, nr. 21) og 22), i forordning (EU) 2019/817 og i henholdsvis artikel 4, nr. 21 og 22, i forordning (EU) 2019/818 er lagret i det fælles identitetsregister.

Artikel 40

Føring af logfiler

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

   a) hvorvidt det var en medlemsstat eller Europol, der fremsatte anmodningen om en forespørgsel; såfremt det var en medlemsstat, der fremsatte anmodningen om en forespørgsel, den pågældende medlemsstat

   b) dato og klokkeslæt for forespørgslen

c) dato og klokkeslæt for svaret

d) de nationale databaser eller Europoldata, hvortil der er sendt en anmodning om en forespørgsel

e) de nationale databaser eller Europoldata, der har givet et svar

f) i givet fald det forhold, at der var en samtidig forespørgsel til det fælles identitetsregister.

2. Hver medlemsstat fører logfiler over forespørgsler, som dens kompetente myndigheders personale, der er behørigt bemyndiget til at anvende routeren, foretager, samt logfiler over forespørgsler, som andre medlemsstater har anmodet om.

Europol fører logfiler over forespørgsler, som dets behørigt bemyndigede personale foretager.

3. De i stk. 1 og 2 omhandlede logfiler må kun anvendes til indsamling af statistikker, til overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, og til sikring af datasikkerhed og -integritet. Disse logfiler beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes tre år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige for overvågningsprocedurerne.

4. Med henblik på overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, har de dataansvarlige adgang til logfilerne til egenkontrol som omhandlet i artikel 55.

Artikel 41

Meddelelsesprocedurer, hvor det er teknisk umuligt at anvende routeren

1. Hvor det er teknisk umuligt at anvende routeren til at foretage forespørgsler i en eller flere nationale databaser eller i Europoldata på grund af routersvigt, underretter eu-LISA på en automatiseret måde de i artikel 35 omhandlede routerbruger. eu-LISA træffer straks foranstaltninger til at afhjælpe det forhold, der gør det teknisk umuligt at anvende routeren.

2. Hvor det er teknisk umuligt at anvende routeren til at foretage forespørgsler i en eller flere nationale databaser på grund af svigt i den nationale infrastruktur i en medlemsstat, underretter den pågældende medlemsstat de øvrige medlemsstater, Kommissionen, eu-LISA og Europol på en automatiseret måde. Den pågældende medlemsstat træffer straks passende foranstaltninger til at afhjælpe det forhold, der gør det teknisk umuligt at anvende routeren.

3. Hvor det er teknisk umuligt at anvende routeren til at foretage forespørgsler i Europoldata på grund af svigt i Europols infrastruktur, underretter Europol medlemsstaterne, Kommissionen og eu-LISA på en automatiseret måde. Europol træffer straks passende foranstaltninger til at afhjælpe det forhold, der gør det teknisk umuligt at anvende routeren.

AFSNIT 2

EPRIS

Artikel 42

EPRIS

1. Det europæiske politiregisterindekssystem (EPRIS) oprettes hermed. Til automatiseret søgning i nationale politiregisterindekser omhandlet i artikel 26 anvender medlemsstaterne og Europol EPRIS.

2. EPRIS består af:

   a) en decentraliseret infrastruktur i medlemsstaterne, herunder et søgeværktøj, der muliggør samtidige forespørgsler i nationale politiregisterindekser baseret på nationale databaser

   b) en central infrastruktur, som understøtter søgeværktøjet og som muliggør samtidige forespørgsler i nationale politiregisterindekser

   c) en sikker kommunikationskanal mellem den centrale infrastruktur, medlemsstaterne og Europol.

Artikel 43

Anvendelse af EPRIS

1. Med henblik på søgning i nationale politiregisterindekser via EPRIS anvendes mindst to af følgende datasæt:

   a) fornavn eller fornavne

   b) efternavn eller efternavne

   c) fødselsdato.

2. Følgende datasæt kan også anvendes, hvor de foreligger:

   a) kaldenavn eller kaldenavne og tidligere anvendt navn eller tidligere anvendte navne

   b) nationalitet eller nationaliteter

   c) fødeland

   d) køn.

3. De data, der er omhandlet i stk. 1, litra a) og b), og stk. 2, litra a), skal være pseudonymiserede.

Artikel 44

Processer

1. Hvor en medlemsstat eller Europol anmoder om en forespørgsel, skal den eller det indsende de data, der er omhandlet i artikel 43.

   EPRIS sender anmodningen om en forespørgsel til medlemsstaternes nationale politiregisterindekser med de data, som den anmodende medlemsstat eller Europol har indsendt, og i overensstemmelse med denne forordning.

2. Ved modtagelse af anmodningen om en forespørgsel fra EPRIS iværksætte hver af de anmodede medlemsstater straks en forespørgsel i deres nationale politiregistre på en automatiseret måde.

3. Eventuelle match, der opstår som følge af forespørgsler som omhandlet i stk. 1 i hver anmodet medlemsstats politiregisterindekser, sendes på en automatiseret måde tilbage til EPRIS.

4. EPRIS returnerer listen over match til den anmodende medlemsstat eller Europol på en automatiseret måde. Listen over match skal angive matchets kvalitet og den medlemsstat eller de medlemsstater, hvis politiregisterindekser indeholder data, der har ført til matchet eller matchene.

5. Efter modtagelse af listen over match beslutter den anmodende medlemsstat, hvilke match det er nødvendigt at følge op på, og sender en begrundet opfølgningsanmodning med de data, der er omhandlet i artikel 25 og 27, og eventuelle yderligere relevante oplysninger til den anmodede medlemsstat eller de anmodede medlemsstater via SIENA. Den anmodede medlemsstat eller de anmodede medlemsstater behandler straks sådanne anmodninger for at beslutte, hvorvidt de vil dele de data, der er lagret i dens eller deres database.

6. Kommissionen vedtager gennemførelsesretsakter, der angiver den tekniske procedure for forespørgsler fra EPRIS i medlemsstaternes politiregisterindekser og formatet for og det maksimale antal svar. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 45

Føring af logfiler

1. Hver deltagende medlemsstat og Europol fører logfiler over alle databehandlingsaktiviteter i EPRIS. Disse logfiler omfatter følgende:

   a) hvorvidt det var en medlemsstat eller Europol, der fremsatte anmodningen om en forespørgsel; såfremt det var en medlemsstat, der fremsatte anmodningen om en forespørgsel, den pågældende medlemsstat

   b) dato og klokkeslæt for forespørgslen

   c) dato og klokkeslæt for svaret

d) de nationale databaser, hvortil en forespørgsel blev sendt

e) de nationale databaser, der gav et svar.

2. Hver deltagende medlemsstat fører logfiler over de anmodninger om forespørgsler, som dens kompetente myndigheders personale, der er behørigt bemyndiget til at anvende EPRIS, foretager. Europol fører logfiler over anmodninger om forespørgsler, som dets behørigt bemyndigede personale foretager.

3. De i stk. 1 og 2 omhandlede logfiler må kun anvendes til indsamling af statistikker, til overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, og til at sikring af datasikkerhed og -integritet. Disse logfiler beskyttes ved hjælp af passende foranstaltninger mod uautoriseret adgang og slettes tre år efter deres oprettelse. Er de imidlertid nødvendige for overvågningsprocedurer, som allerede er indledt, slettes de, når de ikke længere er nødvendige for overvågningsprocedurerne.

4. Med henblik på overvågning af databeskyttelse, herunder kontrol af antageligheden af en forespørgsel og lovligheden af databehandling, har de dataansvarlige adgang til logfilerne til egenkontrol som omhandlet i artikel 55.

Artikel 46

Meddelelsesprocedurer, hvor det er teknisk umuligt at anvende EPRIS

1. Hvor det er teknisk umuligt at anvende EPRIS til at foretage forespørgsler i en eller flere nationale politiregisterindekser på grund af svigt i Europols infrastruktur, underretter Europol medlemsstaterne på en automatiseret måde. Europol træffer straks foranstaltninger til at afhjælpe det forhold, der gør det teknisk umuligt at anvende EPRIS.

2. Hvor det er teknisk umuligt at anvende EPRIS til at foretage forespørgsler i en eller flere nationale politiregisterindekser på grund af svigt i den nationale infrastruktur i en medlemsstat, underretter den pågældende medlemsstat de øvrige medlemsstater, Kommissionen og Europol på en automatiseret måde. Medlemsstaterne træffer straks foranstaltninger til at afhjælpe det forhold, der gør det teknisk umuligt at anvende EPRIS.

Kapitel 4
Udveksling af data efter et match

Artikel 47

Udveksling af centrale data

1. Et sæt af centrale data returneres via routeren inden for 48 timer, efter at alle følgende betingelser er opfyldt:

   a) De procedurer, der er omhandlet i artikel 6, 11 eller 20, viser et match mellem de data, der anvendes til søgningen, og de data, der lagres i den anmodede medlemsstats eller de anmodede medlemsstaters database.

   b) En kvalificeret medarbejder i den anmodende medlemsstat, jf. artikel 6, stk. 6, artikel 11, stk. 2 og artikel 20, stk. 2, eller, i tilfælde af DNA-profiler omhandlet i artikel 6, stk. 7, i den anmodede medlemsstats nationale kontaktpunkt har manuelt bekræftet det i dette stykkes litra a) omhandlede match.

c) Den anmodende medlemsstat eller, i tilfælde af DNA-profiler omhandlet i artikel 6, stk. 7, den anmodede medlemsstat har videregivet en beskrivelse af kendsgerningerne og en angivelse af den tilgrundliggende lovovertrædelse ved brug af den fælles tabel over lovovertrædelser, der er fastsat i en gennemførelsesretsakt, der skal vedtages i henhold til artikel 11b, stk. 1, litra a), i rammeafgørelse 2009/315/RIA, med henblik på at vurdere anmodningens forholdsmæssighed, herunder alvoren af den lovovertrædelse, for hvilken søgningen blev foretaget, i overensstemmelse med national ret i den medlemsstat, der leverer sættet af centrale data.

2. Hvor en medlemsstat i henhold til dens nationale ret først kan levere et særligt sæt af centrale data efter at have indhentet en retskendelse, kan medlemsstaten fravige de frister, der er fastsat i stk. 1, i det omfang, det er nødvendigt for at indhente en sådan kendelse.

3. Det i denne artikels stk. 1 omhandlede sæt af centrale data returneres af den anmodede medlemsstat eller, i tilfælde af DNA-profiler omhandlet i artikel 6, stk. 7, af den anmodende medlemsstat.

4. Hvor det bekræftede match vedrører identificerede data for en person, skal det i stk. 1 omhandlede sæt af centrale data indeholde følgende data, i det omfang de foreligger:

a) fornavn eller fornavne

b) efternavn eller efternavne

c) kaldenavn eller kaldenavne og tidligere anvendt navn eller tidligere anvendte navne

d) fødselsdato

e) nationalitet eller nationaliteter

f) fødeby og -land

g) køn

h) den dato og det sted, hvor de biometriske data blev indsamlet

i) den strafbare handling, med hensyn til hvilken de biometriske data blev indsamlet

j) straffesagsnummeret

k) den kompetente myndighed, der er ansvarlig for straffesagen.

5. Hvor det bekræftede match vedrører uidentificerede data eller spor, skal det i stk. 1 omhandlede sæt af centrale data, indeholde følgende data, i det omfang de foreligger:

a) den dato og det sted, hvor de biometriske data blev indsamlet

b) den strafbare handling, med hensyn til hvilken de biometriske data blev indsamlet

c) straffesagsnummeret

d) den kompetente myndighed, der er ansvarlig for straffesagen.

6. Beslutningen om, hvorvidt den anmodede medlemsstat eller, i tilfælde af DNA-profiler omhandlet i artikel 6, stk. 7, den anmodende medlemsstat skal returnere centrale data, træffes af et menneske.

Kapitel 5
Europol

Artikel 48

Medlemsstaternes adgang til biometriske data, der er meddelt af tredjelande og lagret hos Europol

1. Medlemsstaterne har i overensstemmelse med forordning (EU) 2016/794 adgang til og kan søge via routeren i biometriske data, som tredjelande har meddelt Europol, med henblik på artikel 18, stk. 2, litra a), b) og c), i forordning (EU) 2016/794.

2. Hvor en søgning som omhandlet i stk. 1 resulterer i et match mellem de data, der anvendes til søgningen, og data, der er meddelt af tredjelande og lagret hos Europol, finder opfølgningen sted i overensstemmelse med forordning (EU) 2016/794.

Artikel 49

Europols adgang til data lagret i medlemsstaternes databaser med data meddelt af tredjelande

1. Hvor det er nødvendigt for at nå målsætningerne i artikel 3 i forordning (EU) 2016/794, har Europol i overensstemmelse med nævnte forordning og nærværende forordning adgang til data, som medlemsstaterne lagrer i deres nationale databaser, og politiregisterindekser.

2. Europols forespørgsler, der foretages med biometriske data som søgekriterium, foretages ved brug af routeren.

3. Europols forespørgsler, der foretages med køretøjsregistreringsdata som søgekriterium, foretages ved brug af Eucaris.

4. Europols forespørgsler, der foretages med mistænktes og dømte personers biografiske data som omhandlet i artikel 25 som søgekriterium, foretages ved brug af EPRIS.

5. Europol foretager kun søgninger med data, som er meddelt af tredjelande, i overensstemmelse med denne artikels stk. 1-4, hvor det er nødvendigt for, at det kan udføre sine opgaver med henblik på artikel 18, stk. 2, litra a) og c), i forordning (EU) 2016/794.

6. Hvor de procedurer, der er omhandlet i artikel 6, 11 eller 20, viser et match mellem de data, der er anvendt til søgningen, og data i den anmodede medlemsstats eller de anmodede medlemsstaters nationale database, underretter Europol kun den berørte medlemsstat eller de berørte medlemsstater.

   Den anmodede medlemsstat beslutter, hvorvidt der skal returneres et sæt centrale data via routeren, inden for 48 timer, efter at alle følgende betingelser er opfyldt:

   a) En kvalificeret Europol-medarbejder har manuelt bekræftet et match.

b) Europol har videregivet en beskrivelse af kendsgerningerne og en angivelse af den tilgrundliggende lovovertrædelse ved hjælp af den fælles tabel lovovertrædelser, der er fastsat i en gennemførelsesretsakt, der skal vedtages i henhold til artikel 11b, stk. 1, litra a), i rammeafgørelse 2009/315/RIA, med henblik på at vurdere anmodningens forholdsmæssighed, herunder alvoren af den lovovertrædelse, for hvilken søgningen blev foretaget, i overensstemmelse med national ret i den medlemsstat, der leverer sættet af centrale data.

c) Navnet på det tredjeland, som meddelte dataene, er blevet videregivet.

Hvor en medlemsstat i henhold til dens national ret først kan levere et særligt sæt af centrale data efter at have indhentet en retskendelse, kan medlemsstaten fravige de frister, der er fastsat i stk. 2, i det omfang, det er nødvendigt for at indhente en sådan kendelse.

Hvor det bekræftede match vedrører identificerede data for en person, skal det i stk. 2 omhandlede sæt af centrale data indeholde følgende data, i det omfang de foreligger:

a) fornavn eller fornavne

b) efternavn eller efternavne

c) kaldenavn eller kaldenavne og tidligere anvendt navn eller tidligere anvendte navne

d) fødselsdato

e) nationalitet eller nationaliteter

f) fødeby og -land

g) køn

h) den dato og det sted, hvor de biometriske data blev indsamlet

i) den strafbare handling, med hensyn til hvilken de biometriske data blev indsamlet

j) straffesagsnummeret

k) den kompetente myndighed, der er ansvarlig for straffesagen.

Hvor det bekræftede match vedrører uidentificerede data eller spor, skal det i stk. 2 omhandlede sæt af centrale data indeholde følgende data, i det omfang de foreligger:

a) den dato og det sted, hvor de biometriske data blev indsamlet

b) den strafbare handling, med hensyn til hvilken de biometriske data blev indsamlet

c) straffesagsnummeret

d) den kompetente myndighed, der er ansvarlig for straffesagen.

Beslutningen om, hvorvidt den anmodede medlemsstat skal returnere centrale data, træffes af et menneske.

7. Europols anvendelse af oplysninger, der er fremkommet ved en forespørgsel i henhold til denne artikel og ved udveksling af et sæt af centrale data i overensstemmelse med stk. 6, er betinget af samtykke fra den medlemsstat, i hvis database matchet fandt sted. Hvor medlemsstaten giver tilladelse til at benytte sådanne oplysninger, er Europols behandling reguleres af forordning (EU) 2016/794.

Kapitel 6
Databeskyttelse

Artikel 50

Formålet med databehandlingen

1. Behandling af personoplysninger modtaget af en medlemsstat eller Europol er kun tilladt til de formål, hvortil dataene blev videregivet af den medlemsstat, der leverede dataene i overensstemmelse med denne forordning. Behandling til andre formål er kun tilladt efter forudgående tilladelse fra den medlemsstat, der leverede dataene.

2. Behandling af data leveret af en medlemsstat eller Europol i medfør af artikel 6, 11, 16, 20 eller 26 er kun tilladt, hvor det er nødvendigt med henblik på at:

   a) fastslå, hvorvidt de sammenlignede DNA-profiler, fingeraftryksdata, køretøjsregistreringsdata, ansigtsbilleder eller politiregistre matcher

   b) udveksle et sæt af centrale data i overensstemmelse med artikel 47

   c) udarbejde og indgive en politi- eller retsanmodning om retlig bistand, hvor disse data matcher

   d) føring af logfiler som fastsat i artikel 18, 40 og 45.

3. De data, som en medlemsstat eller Europol modtager, slettes umiddelbart efter automatiserede svar på søgninger, medmindre yderligere behandling er nødvendig med henblik på de formål, der er omhandlet i stk. 2, eller er tilladt i overensstemmelse med stk. 1.

4. Medlemsstaterne foretager, inden de forbinder deres nationale databaser med routeren eller EPRIS, en konsekvensanalyse vedrørende databeskyttelse som omhandlet i artikel 27 i direktiv (EU) 2016/680 og, hvor det er relevant, hører tilsynsmyndigheden som fastsat i nævnte direktivs artikel 28. Tilsynsmyndigheden kan anvende alle de beføjelser, der er omhandlet i artikel 47 i nævnte direktiv, i overensstemmelse med nævnte direktivs artikel 28, stk. 5.

Artikel 51

Nøjagtighed, relevans og lagring af data

1. Medlemsstaterne og Europol sikrer nøjagtigheden og relevansen af personoplysninger, der behandles i medfør af denne forordning. Hvor en medlemsstat eller Europol bliver opmærksom på, at der er blevet leveret data, som er ukorrekte eller ikke længere er ajourførte, eller som ikke burde have været leveret, meddeles dette uden unødigt ophold til den medlemsstat, der modtog dataene, eller til Europol. Alle berørte medlemsstater eller Europol skal uden unødigt ophold berigtige eller slette dataene i overensstemmelse hermed. Hvor den medlemsstat, der modtog dataene, eller Europol har grund til at tro, at de leverede data er ukorrekte eller bør slettes, underretter den eller det den medlemsstat, der har leveret dataene, uden unødigt ophold.

2. Medlemsstaterne og Europol indfører passende foranstaltninger til ajourføring af de data, der er relevante med henblik på denne forordning.

3. Hvor en registreret bestrider nøjagtigheden af data, som en medlemsstat eller Europol er i besiddelse af, hvor den pågældende medlemsstat eller Europol ikke kan fastslå nøjagtigheden på pålidelig vis, og hvor den registrerede anmoder herom, forsynes de pågældende data med en påtegning. Hvor der findes en sådan påtegning, må medlemsstaterne eller Europol kun fjerne den med den registreredes tilladelse eller på grundlag af en afgørelse truffet af den kompetente domstol, den nationale tilsynsmyndighed eller Den Europæiske Tilsynsførende for Databeskyttelse, alt efter hvad der er relevant.

4. Data, der ikke skulle have været leveret eller modtaget, slettes. Retmæssigt leverede og modtagne data slettes:

   a) hvor de ikke eller ikke længere er nødvendige til det formål, hvortil de er leveret

   b) efter udløbet af den maksimale periode for opbevaring af data fastsat i den nationale ret i den medlemsstat, der har leveret dataene, hvor denne medlemsstat har underrettet den medlemsstat, der har modtaget dataene, eller Europol om denne maksimale periode på tidspunktet for levering af dataene, eller

   c) efter udløbet af den maksimale periode for opbevaring af data fastsat i forordning (EU) 2016/794.

Hvor der er grund til at tro, at sletningen af data vil være til skade for den registreredes interesser, begrænses behandlingen af disse data i stedet for sletning. Hvor behandlingen af data er blevet begrænset, må dataene kun behandles til det formål, der forhindrede deres sletning.

Artikel 52

Databehandler

1. eu-LISA er databehandler i den i artikel 3, nr. 12), i forordning (EU) 2018/1725 anvendte betydning i forbindelse med behandling af personoplysninger via routeren.

2. Europol er databehandler i den i artikel 3, nr. 12), i forordning (EU) 2018/1725 anvendte betydning i forbindelse med behandling af personoplysninger via EPRIS.

Artikel 53

Databehandlingssikkerhed

1. Medlemsstaternes kompetente myndigheder, eu-LISA og Europol sørger for sikkerheden af behandlingen af personoplysninger i henhold til denne forordning. Medlemsstaternes kompetente myndigheder, eu-LISA og Europol samarbejder om sikkerhedsrelaterede opgaver.

2. Uden at det berører artikel 33 i forordning (EU) 2018/1725 og artikel 32 i forordning (EU) 2016/794, træffer eu-LISA og Europol de nødvendige foranstaltninger til at sørge for sikkerheden af henholdsvis routeren og EPRIS og for deres tilhørende kommunikationsinfrastruktur.

3. eu-LISA træffer de nødvendige foranstaltninger vedrørende routeren, og Europol træffer de nødvendige foranstaltninger vedrørende EPRIS, med henblik på at:

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

b) forhindre personer uden bemyndigelse i at få adgang til databehandlingsudstyr og -installationer

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

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

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

f) forhindre personer uden bemyndigelse i at bruge automatiserede databehandlingssystemer ved anvendelse af datakommunikationsudstyr

g) sikre, alene ved hjælp af individuelle brugeridentiteter og fortrolige adgangsmetoder, at personer, der er bemyndiget til at have adgang til routeren eller EPRIS, alt efter hvad der er relevant, kun har adgang til de data, der er omfattet af deres bemyndigelse til adgang

h) sikre, at det er muligt at kontrollere og fastslå, til hvilke organer personoplysninger kan leveres ved brug af datatransmissionsudstyr

i) sikre, at det er muligt at kontrollere og fastslå, hvilke data der er blevet behandlet i routeren eller EPRIS, alt efter hvad der er relevant, og hvornår, af hvem og til hvilket formål de er blevet behandlet

j) forhindre uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger under overførsel af personoplysninger til eller fra routeren eller EPRIS, alt efter hvad der er relevant, eller under transport af datamedier, navnlig ved hjælp af passende krypteringsteknikker

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

l) sikre pålidelighed ved at sørge for, at eventuelle funktionsfejl i routeren eller EPRIS, alt efter hvad der er relevant, indberettes behørigt

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

De nødvendige foranstaltninger omhandlet i første afsnit omfatter en sikkerhedsplan, en driftskontinuitetsplan og en katastrofeberedskabsplan

Artikel 54

Sikkerhedshændelser

1. Enhver hændelse, der har eller kan have indvirkning på sikkerheden af routeren eller EPRIS og kan forårsage skade på eller tab af data lagret i, anses for at være en sikkerhedshændelse, især hvor der kan have været uautoriseret adgang til data, eller hvor tilgængeligheden, integriteten og fortroligheden af data er eller kan være blevet bragt i fare.

2. I tilfælde af en sikkerhedshændelse, der vedrører routeren, samarbejder eu-LISA og de berørte medlemsstater eller, i givet fald, Europol med hinanden med henblik på at sikre en hurtig, effektiv og passende reaktion.

3. I tilfælde af en sikkerhedshændelse, der vedrører EPRIS, samarbejder de berørte medlemsstater og Europol med hinanden med henblik på at sikre en hurtig, effektiv og passende reaktion.

4. Medlemsstaterne underretter uden unødigt ophold deres kompetente myndigheder om eventuelle sikkerhedshændelser.

Uden at det berører artikel 92 i forordning (EU) 2018/1725 og i tilfælde af en sikkerhedshændelse, der vedrører routerens centrale infrastruktur, underretter eu-LISA cybersikkerhedstjenesten for Unionens institutioner, organer, kontorer og agenturer (CERT-EU) om væsentlige cybertrusler, væsentlige sårbarheder og væsentlige hændelser uden unødigt ophold og under alle omstændigheder senest 24 timer efter, at eu-LISA er blevet bekendt med dem. Anvendelige og relevante tekniske detaljer om cybertrusler, sårbarheder og hændelser, der gør det muligt at foretage proaktiv opsporing, reagere på hændelser eller træffe afhjælpende foranstaltninger, skal uden unødigt ophold meddeles til CERT-EU.

Uden at det berører artikel 34 i forordning (EU) 2016/794 og artikel 92 i forordning (EU) 2018/1725 og i tilfælde af en sikkerhedshændelse, der vedrører EPRIS' centrale infrastruktur, underretter Europol CERT-EU om væsentlige cybertrusler, væsentlige sårbarheder og væsentlige hændelser uden unødigt ophold og under alle omstændigheder senest 24 timer efter, at Europol er blevet bekendt med dem. Anvendelige og relevante tekniske detaljer om cybertrusler, sårbarheder og hændelser, der gør det muligt at foretage proaktiv opsporing, reagere på hændelser eller træffe afhjælpende foranstaltninger, skal uden unødigt ophold meddeles til CERT-EU.

5. De berørte medlemsstater og EU-agenturer giver straks oplysninger til medlemsstaterne og Europol om en sikkerhedshændelse, der har eller kan have indvirkning på routerens drift eller på tilgængeligheden, integriteten og fortroligheden af dataene, og der rapporteres herom i overensstemmelse med den hændelsesstyringsplan, som eu-LISA skal udforme.

6. De berørte medlemsstater og EU-agenturer giver straks oplysninger til medlemsstaterne om en sikkerhedshændelse, der har eller kan have indvirkning på EPRIS' drift eller på tilgængeligheden, integriteten og fortroligheden af dataene, og der rapporteres herom i overensstemmelse med den hændelsesstyringsplan, som Europol skal udforme.

Artikel 55

Egenkontrol

1. Medlemsstaterne sikrer, at enhver myndighed, der har ret til adgang til at anvende Prüm II-rammen, træffer de foranstaltninger, der er nødvendige for at overvåge dets overholdelse af denne forordning, og samarbejder, hvor det er nødvendigt, med tilsynsmyndigheden. Europol træffer de foranstaltninger, der er nødvendige for at overvåge dets overholdelse af denne forordning, og samarbejder, hvor det er nødvendigt, med Den Europæiske Tilsynsførende for Databeskyttelse.

2. De dataansvarlige gennemfører de nødvendige foranstaltninger for effektivt at overvåge, at databehandlingen overholder denne forordning, herunder ved hyppig kontrol af de i artikel 18, 40 og 45 omhandlede logfiler. De samarbejder, hvor det er nødvendigt og i passende omfang, med tilsynsmyndighederne eller med Den Europæiske Tilsynsførende for Databeskyttelse.

Artikel 56

Sanktioner

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

Artikel 57

Ansvar

Hvis en medlemsstat eller, når det foretager forespørgsler i overensstemmelse med artikel 49, Europol ikke overholder sine forpligtelser i henhold til denne forordning og derved forårsager skade på routeren eller EPRIS, er den pågældende medlemsstat eller Europol ansvarlig for sådan skade, medmindre og i det omfang eu-LISA, Europol eller en anden medlemsstat, der er retligt forpligtet af denne forordning, undlod at træffe rimelige foranstaltninger til at forhindre skaden i at ske eller til at begrænse dens omfang.

Artikel 58

Revision ved Den Europæiske Tilsynsførende for Databeskyttelse

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

2. eu-LISA og Europol udleverer de oplysninger, som Den Europæiske Tilsynsførende for Databeskyttelse anmoder om, giver Den Europæiske Tilsynsførende for Databeskyttelse adgang til alle de dokumenter, denne anmoder om, og til deres i artikel 40 og 45 omhandlede logfiler og giver til enhver tid Den Europæiske Tilsynsførende for Databeskyttelse adgang til alle deres lokaler. Dette stykke berører ikke Den Europæiske Tilsynsførende for Databeskyttelses beføjelser i henhold til artikel 58 i forordning (EU) 2018/1725 og, for så vidt angår Europol, i henhold til artikel 43, stk. 3, i forordning (EU) 2016/794.

Artikel 59

Samarbejde mellem tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse

1. Tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse, der hver især handler inden for deres respektive beføjelser, samarbejder aktivt inden for rammerne af deres respektive ansvarsområder for at sikre et koordineret tilsyn med anvendelsen af denne forordning, navnlig hvis Den Europæiske Tilsynsførende for Databeskyttelse eller en tilsynsmyndighed finder store uoverensstemmelser mellem medlemsstaternes praksis eller finder potentielt ulovlige overførsler ved hjælp af kommunikationskanalerne i Prüm II-rammen.

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

3. To år efter idriftsættelsen af routeren og EPRIS og derefter hvert andet år sender Det Europæiske Databeskyttelsesråd en rapport om sine aktiviteter i henhold til denne artikel til Europa-Parlamentet, Rådet, Kommissionen, eu-LISA og Europol. Denne rapport skal indeholde et kapitel om hver medlemsstat, som udarbejdes af den pågældende medlemsstats tilsynsmyndighed.

Artikel 60

Overførsel af personoplysninger til tredjelande og internationale organisationer

En medlemsstat må kun overføre personoplysninger indhentet i henhold til denne forordning til et tredjeland eller en international organisation i overensstemmelse med kapitel V i direktiv (EU) 2016/680, og hvor den anmodede medlemsstat har givet sin tilladelse inden overførslen.

Europol må kun overføre personoplysninger indhentet i henhold til denne forordning til et tredjeland eller en international organisation, hvor betingelserne i artikel 25 i forordning (EU) 2016/794 er opfyldt, og hvor den anmodede medlemsstat har givet sin tilladelse inden overførslen.

Artikel 61

Sammenhæng med andre retsakter om databeskyttelse

Enhver behandling af personoplysninger med henblik på denne forordning foretages i overensstemmelse med dette kapitel og med direktiv (EU) 2016/680 eller forordning (EU) 2018/1725, (EU) 2016/794 eller (EU) 2016/679, alt efter hvad der finder anvendelse.

Kapitel 7
Ansvarsområder

Artikel 62

Ansvaret for passende omhu

Medlemsstaterne og Europol udviser passende omhu ved vurderingen af, om den automatiserede udveksling af data falder ind under formålet med Prüm II-rammen, der er fastsat i artikel 2, og om den opfylder betingelserne deri, navnlig med hensyn til overholdelsen af grundlæggende rettigheder.

Artikel 63

Uddannelse

Medlemsstaternes kompetente myndigheders, tilsynsmyndigheders og Europols bemyndigede personale skal gives tilstrækkelige ressourcer og uddannelse, alt efter hvad der er relevant, herunder i databeskyttelse og nøjagtig gennemgang af match, til at kunne udføre opgaverne i henhold til denne forordning.

Artikel 64

Medlemsstaternes ansvarsområder

1. Hver medlemsstat er ansvarlig for:

   a) forbindelsen til routerens infrastruktur

b) integrationen af sine eksisterende nationale systemer og infrastrukturer med routeren

c) organisationen, forvaltningen, driften og vedligeholdelsen af sin eksisterende nationale infrastruktur og dens forbindelse til routeren

d) forbindelsen til EPRIS' infrastruktur

e) integrationen af sine eksisterende nationale systemer og sin eksisterende nationale infrastruktur med EPRIS

f) organisationen, forvaltningen, driften og vedligeholdelsen af sin eksisterende nationale infrastruktur og dens forbindelse til EPRIS

g) forvaltningen af og ordningerne for adgangen for sine kompetente myndigheders behørigt bemyndigede personale til routeren i overensstemmelse med denne forordning og oprettelsen og den regelmæssige ajourføring af en liste over disse medarbejdere og deres profiler

h) forvaltningen af og ordningerne for adgangen for sine kompetente myndigheders behørigt bemyndigede personale til EPRIS i overensstemmelse med denne forordning og oprettelsen og den regelmæssige ajourføring af en liste over disse medarbejdere og deres profiler

i) forvaltningen af og ordningerne for adgangsretten for sine kompetente myndigheders behørigt bemyndigede personale til Eucaris i overensstemmelse med denne forordning og oprettelsen og den regelmæssige ajourføring af en liste over disse medarbejdere og deres profiler

j) den manuelle bekræftelse af et match, foretaget af kvalificeret personale, som omhandlet i artikel 6, stk. 6, artikel 6, stk. 7, artikel 11, stk. 2, og artikel 20, stk. 2

k) sikring af tilgængeligheden af de data, der er nødvendige for udveksling af data i overensstemmelse med artikel 5, 10, 16, 19 og 25

l) udveksling af oplysninger i overensstemmelse med artikel 6, 11, 16, 20 og 26

m) berigtigelse, ajourføring eller sletning af data, der er modtaget fra en anmodet medlemsstat, inden for 48 timer efter meddelelsen fra den anmodede medlemsstat om, at de indsendte data var ukorrekte, ikke længere er ajourførte eller var overført ulovligt

n) overholdelse af de datakvalitetskrav, der er fastsat i denne forordning.

2. Hver medlemsstat er ansvarlig for at forbinde sine kompetente myndigheder med routeren, EPRIS og Eucaris.

Artikel 65

Europols ansvarsområder

1. Europol er ansvarligt for forvaltningen af og ordningerne for dets behørigt bemyndigede personales adgang til routeren, EPRIS og Eucaris i overensstemmelse med denne forordning.

2. Europol er ansvarligt for routerens behandling af forespørgsler om Europoldata. Europol tilpasser sine informationssystemer i overensstemmelse hermed.

3. Europol er ansvarligt for enhver teknisk tilpasning af Europols infrastruktur, der er nødvendig for at etablere forbindelsen til routeren og Eucaris.

4. Uden at det berører Europols søgninger i medfør af artikel 49, har Europol ikke adgang til nogen af de personoplysninger, der behandles via EPRIS.

5. Europol er ansvarligt for udviklingen af EPRIS i samarbejde med medlemsstaterne. EPRIS skal tilvejebringe de funktionaliteter, der er fastsat i artikel 42-46.

Europol er ansvarligt for den tekniske forvaltning af EPRIS. Den tekniske forvaltning af EPRIS består af alle de opgaver og tekniske løsninger, der er nødvendige for, at EPRIS' centrale infrastruktur kan fungere og levere uafbrudte tjenester til medlemsstaterne døgnet rundt alle ugens dage i overensstemmelse med denne forordning. Det omfatter den vedligeholdelse og tekniske udvikling, der er nødvendig for at sikre, at EPRIS fungerer på et tilfredsstillende niveau for så vidt angår teknisk kvalitet, særligt hvad angår svartid for indgivelse af anmodninger til de nationale databaser i overensstemmelse med de tekniske specifikationer.

6. Europol sørger for uddannelse i den tekniske anvendelse af EPRIS.

7. Europol er ansvarligt for de procedurer, der er fastsat i artikel 48 og 49.

Artikel 66

eu-LISA's ansvarsområder under routerens udformnings- og udviklingsfase

1. eu-LISA sikrer, at routerens centrale infrastruktur drives i overensstemmelse med denne forordning.

2. Routeren hostes af eu-LISA på dettes tekniske anlæg og leverer de funktionaliteter, der er fastsat i denne forordning, i overensstemmelse med de i artikel 67, stk. 1, omhandlede betingelser for sikkerhed, tilgængelighed, kvalitet og funktionsdygtighed.

3. eu-LISA er ansvarligt for udviklingen af routeren og for eventuelle tekniske tilpasninger, der er nødvendige for routerens drift.

4. eu-LISA har ikke adgang til nogen af de personoplysninger, der behandles gennem routeren.

5. eu-LISA fastlægger udformningen af routerens fysiske arkitektur, herunder dens sikre kommunikationsinfrastruktur og de tekniske specifikationer, og udviklingen heraf for så vidt angår den centrale infrastruktur og den sikre kommunikationsinfrastruktur. eu-LISA's bestyrelse skal godkende udformningen med forbehold af en gunstig udtalelse fra Kommissionen. eu-LISA gennemfører også eventuelle nødvendige tilpasninger af de interoperabilitetskomponenter, der følger af etableringen af routeren som fastsat i denne forordning.

6. eu-LISA udvikler og implementerer routeren hurtigst muligt efter Kommissionens vedtagelse af foranstaltningerne fastsat i artikel 37, stk. 6. Dette udviklingsarbejdet omfatter udarbejdelse og gennemførelse af de tekniske specifikationer, afprøvning og overordnet projektstyring og -koordinering.

7. I udformnings- og udviklingsfasen mødes programstyringsrådet, der er omhandlet i artikel 54 i forordning (EU) 2019/817 og artikel 54 i forordning (EU) 2019/818, regelmæssigt. Den sikrer en hensigtsmæssig forvaltning af routerens udformnings- og udviklingsfase.

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

Den i artikel 78 omhandlede rådgivende gruppe for interoperabilitet mødes regelmæssigt, indtil routeren sættes i drift. Den aflægger efter hvert møde rapport til programstyringsrådet. Den yder teknisk ekspertise til støtte for programstyringsrådets opgaver, og følger op på, hvor langt medlemsstaterne er nået med deres forberedelser.

Artikel 67

eu-LISA's forpligtelser efter routerens idriftsættelse

1. Efter routerens idriftsættelse er eu-LISA ansvarligt for den tekniske forvaltning af routerens centrale infrastruktur, herunder dens vedligeholdelse og teknologiske udvikling. I samarbejde med medlemsstaterne sikrer det på grundlag af en cost-benefit-analyse, at den bedste tilgængelige teknologi anvendes. eu-LISA er også ansvarligt for den tekniske forvaltning af den nødvendige kommunikationsinfrastruktur.

Den tekniske forvaltning af routeren omfatter alle de opgaver og tekniske løsninger, der er nødvendige for, at routeren kan fungere og levere uafbrudte tjenester til medlemsstaterne og Europol døgnet rundt alle ugens dage i overensstemmelse med denne forordning. Den omfatter den vedligeholdelse og tekniske udvikling, der er nødvendig for at sikre, at routeren fungerer på et tilfredsstillende niveau for så vidt angår den tekniske kvalitet, særligt hvad angår tilgængelighed og svartid for indgivelse af anmodninger til de nationale databaser og til Europoldata i overensstemmelse med de tekniske specifikationer.

Routeren udvikles og forvaltes på en sådan måde, at der sikres hurtig, effektiv og kontrolleret adgang, fuldstændig og uafbrudt adgang til routeren og en svartid i overensstemmelse med medlemsstaternes kompetente myndigheders og Europols operationelle behov.

2. Uden at det berører artikel 17 i vedtægten for tjenestemænd i Den Europæiske Union, fastlagt ved Rådets forordning (EØF, Euratom, EKSF) nr. 259/68[18], anvender eu-LISA passende regler for tavshedspligt eller andre tilsvarende fortrolighedskrav i forbindelse med alt personale, der skal arbejde med data, der er lagret i routeren. Denne pligt består fortsat, når de pågældende medarbejdere er fratrådt deres stilling, eller deres virksomhed er ophørt.

   eu-LISA har ikke adgang til nogen af de personoplysninger, der behandles gennem routeren.

3. eu-LISA udfører opgaver vedrørende levering af uddannelse i den tekniske brug af routeren.

---

[18] EUT L 56 af 4.3.1968, s. 1.

Kapitel 8

Ændringer af andre eksisterende instrumenter

Artikel 68

Ændringer af afgørelse 2008/615/RIA og 2008/616/RIA

1. I afgørelse 2008/615/RIA erstattes artikel 1, litra a), artikel 2-6 og afdeling 2 og 3 i kapitel 2 for så vidt angår de medlemsstater, der er bundet af denne forordning, fra datoen for anvendelsen af bestemmelserne i denne forordning vedrørende routeren, der er fastsat i artikel 75, stk. 1. Artikel 1, litra a), artikel 2-6 og afdeling 2 og 3 i kapitel 2 i afgørelse 2008/615/RIA udgår derfor fra datoen for anvendelsen af bestemmelserne i denne forordning vedrørende routeren, der er fastsat i artikel 75, stk. 1.

2. I afgørelse 2008/616/RIA erstattes kapitel 2-5 og artikel 18, 20 og 21 for så vidt angår de medlemsstater, der er bundet af denne forordning, fra datoen for anvendelsen af bestemmelserne i denne forordning vedrørende routeren, der er fastsat i artikel 75, stk. 1. Derfor udgår kapitel 2-5 og artikel 18, 20 og 21 i afgørelse 2008/616/RIA fra datoen for anvendelsen af bestemmelserne i denne forordning vedrørende routeren, der er fastsat i artikel 75, stk. 1.

Artikel 69

Ændring af forordning (EU) 2018/1726

I forordning (EU) 2018/1726 foretages følgende ændringer:

1) Følgende artikel indsættes:

"*Artikel 8d*

Opgaver vedrørende med Prüm II-routeren

I forbindelse med Prüm II-routeren udfører agenturet de opgaver, som det er pålagt ved Europa-Parlamentets og Rådets forordning (EU) …/… [*+].

---

[*] Europa-Parlamentets og Rådets forordning (EU) 2024/… om automatiseret søgning og udveksling af data med henblik på politisamarbejde og om ændring af Rådets afgørelse 2008/615/RIA og 2008/616/RIA og Europa-Parlamentets og Rådets forordning (EU) 2018/1726, (EU) 2019/817 og (EU) 2019/818 (Prüm II-forordningen), (EUT L, …, ELI: …)."

2) Artikel 17, stk. 3, andet afsnit, affattes således:

"Opgaverne vedrørende udvikling og operationel forvaltning, jf. artikel 1, stk. 4 og 5, artikel 3-8 og artikel 8d, 9 og 11, udføres på det tekniske anlæg i Strasbourg, Frankrig."

[+] EUT: Indsæt venligst nummeret på den forordning, der er indeholdt i dokument PE-CONS 75/23 (2021/0410(COD)), i teksten og indsæt nummeret, datoen, titlen og EUT-referencen på nævnte forordning i fodnoten.

3) I artikel 19, nr. 1), foretages følgende ændringer:

a) Følgende litra indsættes:

"eeb) vedtage rapporter om status over udviklingen af Prüm II-routeren i medfør af artikel 80, stk. 2, i forordning (EU) …/…[+]".

b) Litra ff) affattes således:

"ff) vedtage rapporter om den tekniske funktion af følgende:

i) SIS i henhold til artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2018/1861 og artikel 74, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) 2018/1862

ii) VIS i henhold til artikel 50, stk. 3, i forordning (EF) nr. 767/2008 og artikel 17, stk. 3, i afgørelse 2008/633/RIA

iii) ind- og udrejsesystemet i henhold til artikel 72, stk. 4, i forordning (EU) 2017/2226

iv) ETIAS i henhold til artikel 92, stk. 4, i forordning (EU) 2018/1240

v) ECRIS-TCN og ECRIS-referencegennemførelsen i henhold til artikel 36, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) 2019/816

[+] EUT: Indsæt venligst nummeret på den forordning, der er indeholdt i dokument PE-CONS 75/23 (2021/0410(COD)), i teksten.

vi) interoperabilitetskomponenterne i henhold til artikel 78, stk. 3, i forordning (EU) 2019/817 og artikel 74, stk. 3, i forordning (EU) 2019/818

vii) e-CODEX-systemet i henhold til artikel 16, stk. 1, i forordning (EU) 2022/850

viii) JIT-samarbejdsplatformen i henhold til artikel 26, stk. 6, i forordning (EU) 2023/969

ix) Prüm II-routeren i henhold til artikel 80, stk. 5, i forordning (EU) …/…[+]

---

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

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

[+] EUT: Indsæt venligst nummeret på den forordning, der er indeholdt i dokument PE-CONS 75/23 (2021/0410(COD)), i teksten.

c) Litra hh) affattes således:

"hh) vedtage formelle bemærkninger til Den Europæiske Tilsynsførende for Databeskyttelses rapporter om dennes audits i henhold til artikel 56, stk. 2, i forordning (EU) 2018/1861, artikel 42, stk. 2, i forordning (EF) nr. 767/2008, artikel 31, stk. 2, i forordning (EU) nr. 603/2013, artikel 56, stk. 2, i forordning (EU) 2017/2226, artikel 67 i forordning (EU) 2018/1240, artikel 29, stk. 2, i forordning (EU) 2019/816. artikel 52 i forordning (EU) 2019/817 og (EU) 2019/818 og artikel 58, stk. 1, i forordning (EU) …/…[+] og sikre passende opfølgning på disse audits."

[+] EUT: Indsæt venligst nummeret på den forordning, der er indeholdt i dokument PE-CONS 75/23 (2021/0410(COD)), i teksten.

Artikel 70

Ændring af forordning (EU) 2019/817

I artikel 6, stk. 2, i forordning (EU) 2019/817 tilføjes følgende litra:

"d) en sikker kommunikationsinfrastruktur mellem ESP og routeren oprettet ved Europa-Parlamentets og Rådets forordning (EU) …/…[*+].

---

[*] Europa-Parlamentets og Rådets forordning (EU) 2024/… af … om automatiseret søgning og udveksling af data med henblik på politisamarbejde, og om ændring af Rådets afgørelse 2008/615/RIA og 2008/616/RIA og Europa-Parlamentets og Rådets forordning (EU) 2018/1726, (EU) 2019/817 og (EU) 2019/818 (Prüm II-forordningen) (EUT L, …, ELI: …)."

[+] EUT: Indsæt venligst nummeret på den forordning, der er indeholdt i dokument PE-CONS 75/23 (2021/0410(COD)), i teksten og indsæt nummeret, datoen, titlen og EUT-referencen på nævnte forordning i fodnoten.

Artikel 71

Ændring af forordning (EU) 2019/818

I forordning (EU) 2019/818 foretages følgende ændringer:

1) I artikel 6, stk. 2, tilføjes følgende litra:

"d) en sikker kommunikationsinfrastruktur mellem ESP og routeren oprettet ved Europa-Parlamentets og Rådets forordning (EU) …/…[*+].

---

[*] Europa-Parlamentets og Rådets forordning (EU) 2024/… af … om automatiseret søgning og udveksling af data med henblik på politisamarbejde om ændring af Rådets afgørelse 2008/615/RIA og 2008/616/RIA og Europa-Parlamentets og Rådets forordning (EU) 2018/1726, (EU) 2019/817 og (EU) 2019/818 (Prüm II-forordningen), (EUT L, …, ELI: …)."

[+] EUT: Indsæt venligst nummeret på den forordning, der er indeholdt i dokument PE-CONS 75/23 (2021/0410(COD)), i teksten og indsæt nummeret, datoen, titlen og EUT-referencen på nævnte forordning i fodnoten.

2) Artikel 39, stk. 1 og 2, affattes således:

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

2. eu-LISA opretter, gennemfører og hoster CRRS på sine tekniske anlæg, indeholdende de oplysninger og statistikker, der er omhandlet i artikel 74 i forordning (EU) 2018/1862 og artikel 32 i forordning (EU) 2019/816, og som holdes logisk adskilt af EU-informationssystemet. eu-LISA indsamler også oplysninger og statistikker fra den router, der er omhandlet i artikel 72, stk. 1, i forordning (EU) …/…[+]. Der gives adgang til CRRS via en kontrolleret og sikret adgang og særlige brugerprofiler, udelukkende med henblik på rapportering og statistikker, til de myndigheder, der er omhandlet i artikel 74 i forordning (EU) 2018/1862, artikel 32 i forordning (EU) 2019/816 og artikel 72, stk. 1, i forordning (EU) …/…[+]."

[+] EUT: Indsæt venligst nummeret på den forordning, der er indeholdt i dokument-PE-CONS 75/23 (2021/0410(COD)), i teksten.

Kapitel 9
Afsluttende bestemmelser

Artikel 72

Rapportering og statistik

1. Hvor det er nødvendigt, har de behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen, eu-LISA og Europol adgang til følgende data vedrørende routeren, udelukkende med henblik på rapportering og statistik:

   a) antal forespørgsler pr. medlemsstat og antal forespørgsler fra Europol pr. datakategori

   b) antal forespørgsler til hver af de forbundne databaser

   c) antal match med hver medlemsstats database pr. datakategori

   d) antal match med Europoldata pr. datakategori

   e) antal bekræftede match, hvor der blev udvekslet centrale data

   f) antal bekræftede match, hvor der ikke blev udvekslet centrale data

   g) antal forespørgsler til det fælles identitetsregister via routeren, og

h) antal match pr. type som følger:

i) identificerede data (person) – uidentificerede data (spor)

ii) uidentificerede data (spor) – identificerede data (person)

iii) uidentificerede v (spor) – uidentificerede data (spor)

iv) identificerede data (person) – identificerede data (person).

Det må ikke være muligt at identificere enkeltpersoner ud fra dataene anført i første afsnit.

2. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og Europol har adgang til følgende data vedrørende Eucaris, udelukkende med henblik på rapportering og statistik:

a) antal forespørgsler pr. medlemsstat og antal forespørgsler fra Europol

b) antal forespørgsler til hver af de forbundne databaser, og

c) antal match med hver medlemsstats database.

Det må ikke være muligt at identificere enkeltpersoner ud fra dataene anført i første afsnit.

3. De behørigt bemyndigede medarbejdere hos medlemsstaternes kompetente myndigheder, Kommissionen og Europol har adgang til følgende data vedrørende EPRIS, udelukkende med henblik på rapportering og statistik:

a) antal forespørgsler pr. medlemsstat og antal forespørgsler fra Europol

b) antal forespørgsler til hvert af de forbundne indekser, og

c) antal match med hver medlemsstats database.

Det må ikke være muligt at identificere enkeltpersoner ud fra dataene anført i første afsnit.

4. eu-LISA lagrer de data, der er anført i denne artikels stk. 1, i det centrale register for rapportering og statistik, som er oprettet ved artikel 39 i forordning (EU) 2019/818. Europol lagrer de data, der er anført i denne artikels stk. 3. Disse data skal gøre det muligt for medlemsstaternes kompetente myndigheder, Kommissionen, eu-LISA og Europol at indhente rapporter og statistikker, der kan tilpasses, for at øge effektiviteten af retshåndhævelsessamarbejde.

Artikel 73

Omkostninger

1. Omkostninger i forbindelse med etablering og drift af routeren og EPRIS afholdes over Unionens almindelige budget.

2. Omkostninger i forbindelse med integration af eksisterende nationale infrastruktur og denne forbindelse til routeren og EPRIS samt omkostninger i forbindelse med oprettelsen af nationale databaser over ansigtsbilleder og nationale politiregisterindekser til forebyggelse, afsløring og efterforskning af strafbare handlinger afholdes over Unionens almindelige budget.

   Følgende omkostninger dækkes ikke:

   a) medlemsstaternes projektstyringskontor (møder, tjenesterejser, kontorer)

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

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

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

3. Hver medlemsstat afholder omkostningerne i forbindelse med forvaltning, anvendelse og vedligeholdelse af Eucaris.

4. Hver medlemsstat afholder omkostningerne i forbindelse med forvaltning, anvendelse og vedligeholdelse af deres forbindelser til routeren og EPRIS.

Artikel 74

Underretninger

1. Medlemsstaterne underretter eu-LISA om de kompetente myndigheder, der er omhandlet i artikel 36. Disse myndigheder kan anvende eller få adgang til routeren.

2. eu-LISA underretter Kommissionen, når de test, der er omhandlet i artikel 75, stk. 1, litra b), er afsluttet på tilfredsstillende vis.

3. Europol underretter Kommissionen, når de test, der er omhandlet i artikel 75, stk. 3, litra b), er afsluttet på tilfredsstillende vis.

4. Hver medlemsstat underretter de øvrige medlemsstater, Kommissionen, eu-LISA og Europol om det indhold i deres nationale DNA-databaser og de betingelser for automatiserede søgninger, som artikel 5 og 6 finder anvendelse på.

5. Hver medlemsstat underretter de øvrige medlemsstater, Kommissionen, eu-LISA og Europol om det indhold i deres nationale fingeraftryksdatabaser og de betingelser for automatiserede søgninger, som artikel 10 og 11 finder anvendelse på.

6. Hver medlemsstat underretter de øvrige medlemsstater, Kommissionen, eu-LISA og Europol om det indhold i deres nationale databaser over ansigtsbilleder og de betingelser for automatiserede søgninger, som artikel 19 og 20 finder anvendelse på.

7. Medlemsstater, der deltager i automatiseret udveksling af politiregistre i medfør af artikel 25 og 26, underretter de øvrige medlemsstater, Kommissionen og Europol om indholdet af deres nationale politiregisterindekser og af de nationale databaser, der anvendes til at oprette disse indekser, og betingelserne for automatiserede søgninger.

8. Medlemsstaterne underretter Kommissionen, eu-LISA og Europol om deres nationale kontaktpunkt, der er udpeget i henhold til artikel 30. Kommissionen udarbejder en liste over de nationale kontaktpunkter, som den har fået underretning om, og stiller den til rådighed for alle medlemsstater.

Artikel 75

Idriftsættelse

1. Kommissionen fastsætter den dato, fra hvilken medlemsstaterne og Europol kan begynde at anvende routeren ved hjælp af en gennemførelsesretsakt, når følgende betingelser er opfyldt:

   a) foranstaltningerne i artikel 5, stk. 3, artikel 8, stk. 2 og 3, artikel 13, stk. 2 og 3, artikel 17, stk. 3, artikel 22, stk. 2 og 3, artikel 31 og artikel 37, stk. 6, er vedtaget

   b) eu-LISA har meddelt, at den omfattende test af routeren, som det har udført i samarbejde med medlemsstaternes kompetente myndigheder og Europol, er afsluttet på tilfredsstillende vis.

Kommissionen fastsætter ved hjælp af den i første afsnit omhandlede gennemførelsesretsakt den dato, fra hvilken medlemsstaterne og Europol skal begynde at anvende routeren. Denne dato skal ligge et år efter den dato, der er fastsat i overensstemmelse med første afsnit.

Kommissionen kan udsætte den dato, fra hvilken medlemsstaterne og Europol skal begynde at anvende routeren med højst et år, hvis en vurdering af routerens gennemførelse har vist, at en sådan udsættelse er nødvendig.

2. To år efter idriftsættelsen af routeren sikrer medlemsstaterne tilgængeligheden af ansigtsbilleder som omhandlet i artikel 19 med henblik på automatiseret søgning efter ansigtsbilleder som omhandlet i artikel 20.

3. Kommissionen fastsætter den dato, fra hvilken medlemsstaterne og Europol skal begynde at anvende EPRIS, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er opfyldt:

   a) foranstaltningerne i artikel 44, stk. 6, er vedtaget

   b) Europol har meddelt, at den omfattende test af EPRIS, som det har udført i samarbejde med medlemsstaternes kompetente myndigheder, er afsluttet på tilfredsstillende vis.

4. Kommissionen fastsætter den dato, fra hvilken Europol skal stille biometriske data fra tredjelande til rådighed for medlemsstaterne i overensstemmelse med artikel 48, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er opfyldt:

   a) routeren er i drift

   b) Europol har erklæret, at der er gennemført en omfattende test af dets forbindelse til routeren, som det har gennemført i samarbejde med medlemsstaternes kompetente myndigheder og eu-LISA.

5. Kommissionen fastsætter den dato, fra hvilken Europol skal have adgang til data, der er lagret i medlemsstaternes databaser, i overensstemmelse med artikel 49, ved hjælp af en gennemførelsesretsakt, når følgende betingelser er opfyldt:

   a) routeren er i drift

   b) Europol har erklæret, at der er gennemført en omfattende test af dets forbindelse til routeren, som det har gennemført i samarbejde med medlemsstaternes kompetente myndigheder og eu-LISA.

6. De i denne artikel omhandlede gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 77, stk. 2.

Artikel 76

Overgangsbestemmelser og undtagelser

1. Medlemsstaterne og EU-agenturerne begynder at anvende artikel 19-22, artikel 47 og artikel 49, stk. 6, fra den dato, der er fastsat i overensstemmelse med artikel 75, stk. 1, første afsnit, med undtagelse af medlemsstater, der ikke er begyndt at anvende routeren.

2. Medlemsstaterne og EU-agenturerne begynder at anvende artikel 25-28 og artikel 49, stk. 4, fra den dato, der er fastsat i overensstemmelse med artikel 75, stk. 3.

3. Medlemsstaterne og EU-agenturerne begynder at anvende artikel 48 fra den dato, der er fastsat i overensstemmelse med artikel 75, stk. 4.

4. Medlemsstaterne og EU-agenturerne begynder at anvende artikel 49, stk. 1, 2, 3, 5 og 7, fra den dato, der er fastsat i overensstemmelse med artikel 75, stk. 5.

Artikel 77

Udvalgsprocedure

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

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

Artikel 78

Rådgivende gruppe for interoperabilitet

Ansvarsområderne for den rådgivende gruppe for interoperabilitet, der er nedsat ved artikel 75 i forordning (EU) 2019/817 og artikel 71 i forordning (EU) 2019/818, udvides til at omfatte routeren. Denne rådgivende gruppe for interoperabilitet bistår eu-LISA med ekspertise vedrørende routeren, navnlig i forbindelse med udarbejdelsen af dets årlige arbejdsprogram og dets årlige aktivitetsrapport.

Artikel 79

Praktisk håndbog

Kommissionen stiller i tæt samarbejde med medlemsstaterne, eu-LISA, Europol og Den Europæiske Unions Agentur for Grundlæggende Rettigheder en praktisk håndbog til rådighed for gennemførelsen og forvaltningen af denne forordning. Den praktiske håndbog skal indeholde tekniske og operationelle retningslinjer, anbefalinger og bedste praksis. Kommissionen vedtager håndbogen i form af en henstilling inden idriftsættelsen af både routeren og EPRIS. Kommissionen ajourfører den praktiske håndbog regelmæssigt, og når det er nødvendigt.

Artikel 80

Overvågning og evaluering

1. eu-LISA sikrer, at der er indført procedurer til at overvåge udviklingen af routeren i lyset af målene vedrørende planlægning og omkostninger og til at overvåge dets funktion i lyset af målene vedrørende teknisk output, omkostningseffektivitet, sikkerhed og servicekvalitet.

   Europol sikrer, at der er indført procedurer til at overvåge udviklingen af EPRIS i lyset af målene vedrørende planlægning og omkostninger og til at overvåge dets funktion i lyset af målene vedrørende teknisk output, omkostningseffektivitet, sikkerhed og servicekvalitet.

2. Senest den … [ét år efter datoen for denne forordnings ikrafttræden] og derefter hvert år i routerens udviklingsfase forelægger eu-LISA Europa-Parlamentet og Rådet en rapport om status for udviklingen af routeren. Disse rapporter indeholder detaljerede oplysninger om de afholdte omkostninger og oplysninger om eventuelle risici, der kunne have indvirkning på de samlede omkostninger, som skal afholdes over Unionens almindelige budget i medfør af artikel 73.

   Når routeren er færdigudviklet, forelægger eu-LISA Europa-Parlamentet og Rådet en rapport, som i detaljer forklarer, hvordan målene, navnlig vedrørende planlægning og omkostninger, blev opfyldt, og angiver grundene til eventuelle afvigelser.

3. Senest den … [ét år efter datoen for denne forordnings ikrafttræden] og derefter hvert år i EPRIS' udviklingsfase forelægger Europol Europa-Parlamentet og Rådet en rapport om status for udviklingen af EPRIS. Disse rapporter indeholder detaljerede oplysninger om de afholdte omkostninger og oplysninger om eventuelle risici, som kunne påvirke de samlede omkostninger, som skal afholdes over Unionens almindelige budget i medfør af artikel 73.

Når EPRIS er færdigudviklet, forelægger Europol Europa-Parlamentet og Rådet en rapport, som i detaljer forklarer, hvordan målene, navnlig vedrørende planlægning og omkostninger, blev opfyldt, og angiver grundene til eventuelle afvigelser.

4. Med henblik på teknisk vedligeholdelse har eu-LISA adgang til de nødvendige oplysninger om de databehandlingsaktiviteter, der udføres i routeren. Med henblik på den tekniske vedligeholdelse har Europol adgang til de nødvendige oplysninger om de databehandlingsaktiviteter, der udføres i EPRIS.

5. To år efter idriftsættelsen af routeren og derefter hvert andet år forelægger eu-LISA Europa-Parlamentet, Rådet og Kommissionen en rapport om, hvordan routeren teknisk fungerer, herunder dens sikkerhed.

6. To år efter idriftsættelsen af EPRIS og derefter hvert andet år forelægger Europol Europa-Parlamentet, Rådet og Kommissionen en rapport om, hvordan EPRIS teknisk fungerer, herunder dets sikkerhed.

7. Tre år efter idriftsættelsen af routeren og EPRIS som omhandlet i artikel 75 og derefter hvert fjerde år udarbejder Kommissionen en rapport om den samlede evaluering af Prüm II-rammen.

Ét år efter idriftsættelsen af routeren og derefter hvert andet år udarbejder Kommissionen en rapport med en evaluering af brugen af ansigtsbilleder i henhold til denne forordning.

Rapporterne omhandlet i første og andet afsnit skal indeholde følgende:

a) en vurdering af denne forordnings anvendelse, herunder hver medlemsstats og Europols anvendelse af den

b) en undersøgelse af de opnåede resultater set i forhold til denne forordnings mål og dens indvirkning på grundlæggende rettigheder

c) indvirkningen, effektiviteten og virkningsfuldheden af Prüm II-rammens virksomhed og dens arbejdsmetoder set i lyset af dens mål, mandat og opgaver

d) en vurdering af Prüm II-rammens sikkerhed.

Kommissionen fremsender disse rapporter til Europa-Parlamentet, Rådet, Den Europæiske Tilsynsførende for Databeskyttelse og Den Europæiske Unions Agentur for Grundlæggende Rettigheder.

8. I de rapporter, der er omhandlet i stk. 7, første afsnit, skal Kommissionen være særlig opmærksom på følgende nye datakategorier: ansigtsbilleder og politiregistre. Kommissionen inkluderer i sådanne rapporter de enkelte medlemsstaters og Europols anvendelse af disse nye datakategorier og deres betydning, virkningsfuldhed og effektivitet. I de rapporter, der er omhandlet i stk. 7, andet afsnit, skal Kommissionen være særligt opmærksom på risikoen for falske match og på datakvalitet.

9. Medlemsstaterne og Europol sender eu-LISA og Kommissionen de oplysninger, der er nødvendige for at udarbejde de i stk. 2 og 5 omhandlede rapporter. Disse oplysninger må ikke påvirke arbejdsmetoder negativt eller afsløre medlemsstaternes kompetente myndigheders kilder, medarbejdere eller undersøgelser.

10. Medlemsstaterne giver Kommissionen og Europol de oplysninger, der er nødvendige for at udarbejde de i stk. 3 og 6 omhandlede rapporter. Disse oplysninger må ikke påvirke arbejdsmetoder negativt eller afsløre medlemsstaternes kompetente myndigheders kilder, medarbejdere eller undersøgelser.

11. Uden at det berører fortrolighedskrav giver Medlemsstaterne, eu-LISA og Europol Kommissionen de oplysninger, der er nødvendige for at udarbejde de rapporter, der er omhandlet i stk. 7. Medlemsstaterne meddeler også Kommissionen antallet af bekræftede match med hver medlemsstats database pr. datakategori og pr. datatype. Disse oplysninger må ikke påvirke arbejdsmetoder negativt eller afsløre de kompetente myndigheders kilder, medarbejdere eller undersøgelser.

Artikel 81

Ikrafttræden og anvendelse

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

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

Udfærdiget i Strasbourg, den …

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*