EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2018/1861

av 28. november 2018

om opprettelse, drift og bruk av Schengen-informasjonssystemet (SIS) innenfor inn- og utreisekontroller, om endring av konvensjonen om gjennomføring av Schengen-avtalen og om endring og oppheving av forordning (EF) nr. 1987/2006

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR —

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 77 nr. 2 bokstav b) og d), og artikkel 79 nr. 2 bokstav c),

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

etter den ordinære regelverksprosedyren ([1]), og

ut fra følgende betraktninger:

(1) Schengen-informasjonssystemet (SIS) utgjør et grunnleggende verktøy for anvendelse av bestemmelsene i Schengen-regelverket som innarbeidet i Den europeiske union. SIS er et av de viktigste kompenserende tiltak som bidrar til å opprettholde et høyt sikkerhetsnivå innenfor området frihet, sikkerhet og rettferdighet i Unionen ved å støtte operativt samarbeid mellom nasjonale vedkommende myndigheter, særlig grensevakter, politiet, tollmyndigheter, innvandringsmyndigheter og myndigheter med ansvar for å forebygge, avsløre, etterforske eller rettsforfølge straffbare forhold eller fullbyrde strafferettslige sanksjoner.

(2) SIS ble opprinnelig opprettet i henhold til bestemmelsene i avdeling IV i konvensjon av 19. juni 1990 om gjennomføring av Schengen-avtalen av 14. juni 1985 mellom regjeringene i statene i Den økonomiske union Benelux, Forbundsrepublikken Tyskland og Republikken Frankrike om gradvis avskaffelse av kontrollen på de felles grenser ([2]) (konvensjonen om gjennnomføring av Schengen-avtalen). Kommisjonen fikk i oppdrag å utvikle annen generasjon av SIS (SIS II) i henhold til rådsforordning (EF) nr. 2424/2001 ([3]) og rådsbeslutning 2001/886/JIS ([4]). Det ble senere opprettet ved europaparlaments- og rådsforordning (EF) nr. 1987/2006 ([5]) og ved rådsbeslutning 2007/533/JIS ([6]). SIS II erstattet det SIS som ble opprettet i henhold til konvensjonen om gjennomføring om Schengen-avtalen.

(3) Tre år etter at SIS II ble satt i drift, foretok Kommisjonen en evaluering av systemet i samsvar med forordning (EF) nr. 1987/2006 og beslutning 2007/533/JIS. Den 21. desember 2016 framla Kommisjonen for Europaparlamentet og Rådet rapporten om evaluering av annen generasjon av Schengen-informasjonssystemet (SIS II) i samsvar med artikkel 24 nr. 5, artikkel 43 nr. 3 og artikkel 50 nr. 5 i forordning (EF) nr. 1987/2006 og artikkel 59 nr. 3 og artikkel 66 nr. 5 i beslutning 2007/533/JIS og et ledsagende arbeidsdokument. Anbefalingene i disse dokumentene bør gjenspeiles i denne forordning når det er relevant.

(4) Denne forordning utgjør rettsgrunnlaget for SIS med hensyn til spørsmål som omfattes av tredje del avdeling V kapittel 2 i traktaten om Den europeiske unions virkemåte (TEUV). Europaparlaments- og rådsforordning (EU) 2018/1862 ([7]) utgjør rettsgrunnlaget for SIS med hensyn til spørsmål som omfattes av tredje del avdeling V kapittel 4 og 5 i TEUV.

(1) Europaparlamentets holdning av 24. oktober 2018 (ennå ikke offentliggjort i EUT) og rådsbeslutning av 19. november 2018.
(2) EUT L 239 av 22.9.2000, s. 19.
(3) Rådsforordning (EF) nr. 2424/2001 av 6. desember 2001 om utvikling av annen generasjon av Schengen-informasjonssystemet (SIS II) (EUT L 328 av 13.12.2001, s. 4)
(4) Rådsbeslutning 2001/886/JIS av 6. desember 2001 om utvikling av annen generasjon av Schengen-informasjonssystemet (SIS II) (EUT L 328 av 13.12.2001, s. 1).
(5) Europaparlaments- og rådsforordning (EF) nr. 1987/2006 av 20. desember 2006 om opprettelse, drift og bruk av annen generasjon av Schengen-informasjonssystemet (SIS II) (EUT L 381 av 28.12.2006, s. 4).
(6) Rådsbeslutning 2007/533/JIS av 12. juni 2007 om opprettelse, drift og bruk av annen generasjon av Schengen-informasjonssystemet (SIS II) (EUT L 205 av 7.8.2007, s. 63).
(7) Europaparlaments- og rådsforordning (EU) 2018/1862 av 28. november 2018 om opprettelse, drift og bruk av Schengen-informasjonssystemet (SIS) innenfor politisamarbeid og strafferettslig samarbeid, om endring og oppheving av rådsbeslutning 2007/533/JIS og om oppheving av europaparlaments- og rådsforordning (EF) nr. 1986/2006 og kommisjonsbeslutning 2010/261/EU (EUT L 312 av 7.12.2018, s. 56).

(5) Det forhold at rettsgrunnlaget for SIS består av atskilte instrumenter, berører ikke prinsippet om at SIS utgjør ett enkelt informasjonssystem som skal fungere som sådant. Det bør omfatte et enkelt nettverk av nasjonale kontorer, SIRENE-kontorene, for å sikre utveksling av utfyllende opplysninger. Visse bestemmelser i disse instrumentene bør derfor være enslydende.

(6) Det er nødvendig å angi målene for SIS, visse elementer ved systemets tekniske struktur og finansiering, fastsette regler for den gjennomgående driften og bruken av systemet og fastsette ansvarsområder. Det er også nødvendig å fastsette hvilke kategorier av opplysninger som skal registreres i systemet, hvilke formål opplysningene registreres og behandles for, og hvilke kriterier de registreres på. Regler er også nødvendig for å regulere hvordan meldinger skal slettes, hvilke myndigheter som skal ha adgang til opplysningene, hvordan biometriske opplysninger skal brukes, og for å fastsette nærmere regler for personvern og behandling av opplysninger.

(7) Meldinger i SIS inneholder bare informasjon som er nødvendig for å identifisere en person og for å fastsette hvilke tiltak som skal treffes. Medlemsstatene bør derfor utveksle utfyllende opplysninger om meldinger når det er nødvendig.

(8) SIS omfatter et sentralt system (det sentrale SIS II) og nasjonale systemer. De nasjonale systemene kan inneholde en fullstendig eller delvis kopi av SIS-databasen, som kan være felles for to eller flere medlemsstater. Ettersom SIS er det viktigste instrumentet for utveksling av opplysninger i Europa med sikte på å ivareta sikkerhet og effektiv grenseforvaltning, er det nødvendig å sikre uavbrutt drift på både sentralt og nasjonalt plan. SIS' tilgjengelighet bør overvåkes nøye på sentralt plan og medlemsstatsplan, og ethvert tilfelle av manglende tilgjengelighet for sluttbrukere bør registreres og meldes til berørte parter på nasjonalt plan og unionsplan. Hver enkelt medlemsstat bør foreta sikkerhetskopiering av sitt nasjonale system. Medlemsstatene bør også sikre uavbrutt tilgang til det sentrale SIS ved hjelp av dobbelte og fysisk og geografisk atskilte tilkoplingspunkter. Det sentrale SIS og kommunikasjonsinfrastrukturen bør drives slik at det sikres at de fungerer 24 timer i døgnet 7 dager i uken. Derfor bør Den europeiske unions byrå for driftsforvaltning av store IT-systemer innenfor området frihet, sikkerhet og rettferdighet («eu-LISA»), opprettet ved europaparlaments- og rådsforordning (EU) 2018/1726 ([1]), gjennomføre tekniske løsninger for å styrke uavbrutt tilgang til SIS, med forbehold for en uavhengig konsekvensvurdering og nytte- og kostnadsanalyse.

(9) Det må utarbeides en håndbok med detaljerte regler for utveksling av utfyllende opplysninger om tiltak som skal treffes på grunnlag av en melding («SIRENE-håndboken»). SIRENE-kontorene bør sikre at utvekslingen av slike opplysninger skjer raskt og effektivt.

(10) For å sikre effektiv utveksling av utfyllende opplysninger, herunder om de tiltak som skal treffes ifølge meldingene, er det hensiktsmessig å styrke SIRENE-kontorenes funksjon ved å fastsette kravene om tilgjengelige ressurser, brukeropplæring og svartid ved forespørsler fra andre SIRENE-kontorer.

(11) Medlemsstatene bør sikre at personalet ved sitt SIRENE-kontor har de språkferdigheter og den kunnskap om relevant rett og saksbehandlingsregler som er nødvendig for å utføre sine oppgaver.

(12) For å kunne dra full nytte av funksjonene i SIS bør medlemsstatene sikre at sluttbrukerne og SIRENE-kontorenes personale får regelmessig opplæring, herunder i datasikkerhet, personvern og datakvalitet. SIRENE-kontorene bør delta i utviklingen av opplæringsprogrammer. SIRENE-kontorene bør så vidt mulig også utveksle personale med andre SIRENE-kontorer minst én gang i året. Medlemsstatene oppfordres til å treffe egnede tiltak for å unngå at avgangshyppighet fører til kompetanse- og erfaringstap.

(13) eu-LISA sørger for driftsforvaltning av de sentrale delene av SIS. For å gjøre det mulig for eu-LISA å sette av nødvendige økonomiske og personalmessige ressurser for alle aspekter ved driftsforvaltningen av det sentrale SIS og kommunikasjonsinfrastrukturen bør dets oppgaver fastsettes nærmere i denne forordning, særlig når det gjelder de tekniske aspekter ved utvekslingen av utfyllende opplysninger.

(14) Uten at det berører medlemsstatenes ansvar for at opplysninger som registreres i SIS, er riktige, og SIRENE-kontorenes rolle som kvalitetskoordinatorer, bør eu-LISA være ansvarlig for å forbedre datakvaliteten ved å innføre et sentralt kvalitetskontrollverktøy og bør jevnlig framlegge rapporter for

(1) Europaparlaments- og rådsforordning (EU) 2018/1726 av 14. november 2018 om Den europeiske unions byrå for driftsforvaltning av store IT-systemer innenfor området frihet, sikkerhet og rettferdighet (eu-LISA) og om endring av forordning (EF) nr. 1987/2006 og rådsbeslutning 2007/533/JIS og om oppheving av forordning (EU) nr. 1077/2011 (EUT L 295 av 21.11.2018, s. 99).

Kommisjonen og medlemsstatene. Kommisjonen bør framlegge rapport for Europaparlamentet og Rådet om problemer som har oppstått med datakvaliteten. For ytterligere å øke kvaliteten på opplysningene i SIS bør eu-LISA også tilby de nasjonale opplæringsinstitusjonene og i størst mulig grad SIRENE-kontorene og sluttbrukerne opplæring i bruken av SIS.

(15) For å muliggjøre bedre overvåking av bruken av SIS og for å analysere tendenser vedrørende migrasjonspress og grenseforvaltning bør eu-LISA kunne utvikle en avansert metode for statistisk rapportering til medlemsstatene, Europaparlamentet, Rådet, Kommisjonen, Europol og Det europeiske grense- og kystvaktbyrå uten å sette dataintegriteten i fare. Det bør derfor opprettes et sentralt datalager. Statistikk som lagres i eller innhentes fra nevnte datalager, bør ikke inneholde personopplysninger. Medlemsstatene bør oversende statistikk over utøvelse av retten til innsyn, retting av uriktige

opplysninger og sletting av ulovlig lagrede opplysninger i forbindelse med samarbeid mellom tilsynsmyndigheter og EUs datatilsyn i henhold til denne forordning.

(16) Det bør innføres nye opplysningskategorier i SIS for å gjøre det mulig for sluttbrukere å treffe velbegrunnede beslutninger på grunnlag av en melding uten å miste tid. Derfor bør meldinger om nektet innreise og opphold inneholde informasjon om beslutningen som ligger til grunn for meldingen. For å lette identifisering og avsløre flere identiteter bør meldingen dessuten, dersom slike opplysninger er tilgjengelige, inneholde en henvisning til den berørte personens personlige identitetsdokument eller dets nummer og en kopi av dokumentet, om mulig i farger.

(17) Dersom det er absolutt nødvendig, bør vedkommende myndigheter kunne registrere særlig informasjon i SIS om en persons eventuelle særlige objektive fysiske kjennetegn av uforanderlig art, f.eks. tatoveringer, merker eller arr.

(18) Når det opprettes en melding, bør alle relevante opplysninger angis, dersom de er tilgjengelige, særlig den berørte personens fornavn, for å minimere risikoen for falske treff og unødig driftsvirksomhet.

(19) I SIS bør det ikke lagres opplysninger som brukes til å utføre søk, med unntak av logger for å kontrollere at søket er lovlig, overvåke at behandlingen av opplysninger skjer på lovlig måte, utføre egenkontroll og sikre at de nasjonale systemene virker tilfredsstillende samt med sikte på dataintegritet og -sikkerhet.

(20) SIS bør tillate behandling av biometriske opplysninger for å bidra til pålitelig identifisering av berørte personer. Registrering av fotografier, ansiktsbilder eller fingeravtrykksopplysninger i SIS og bruk av slike opplysninger bør begrenses til det som er nødvendig for å oppnå de fastsatte målene, bør være tillatt i henhold til unionsretten, bør overholde de grunnleggende rettigheter, herunder barnets interesse, og bør være i samsvar med unionsretten om personvern, herunder de relevante bestemmelsene om personvern i denne forordning. For å unngå problemer som følge av feilidentifisering bør SIS på samme måte også tillate behandling av opplysninger om personer hvis identitet er misbrukt, med forbehold for egnede vernetiltak, den berørte personens samtykke for hver opplysningskategori, særlig håndflateavtrykk, og en streng begrensning av hvilke formål slike personopplysninger lovlig kan behandles for.

(21) Medlemsstatene bør treffe nødvendige tekniske tiltak for å sikre at sluttbrukere som utfører et berettiget søk i en av de nasjonale politi- eller innvandringsdatabasene, samtidig også søker i SIS, med forbehold for prinsippene i artikkel 4 i europaparlaments- og rådsdirektiv (EU) 2016/680 ([1]) og artikkel 5 i europaparlaments- og rådsforordning (EU) 2016/679 ([2]). Det bør sikre at SIS fungerer som det viktigste kompenserende tiltak innenfor området uten kontroller ved de indre grensene og bedre bidrar til å bekjempe den grenseoverskridende dimensjonen av kriminalitet og kriminelles bevegelighet.

(22) I denne forordning bør det fastsettes vilkår for bruk av fingeravtrykksopplysninger, fotografier og ansiktsbilder til identifisering og kontroll. Ansiktsbilder og fotografier bør for identifisering i første omgang brukes bare ved alminnelige grenseoverganger. Slik bruk bør være gjenstand for en rapport fra Kommisjonen som bekrefter at teknologien er tilgjengelig, pålitelig og klar til bruk.

(1) Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om vern av fysiske personer i forbindelse med vedkommende myndigheters behandling av personopplysninger for å forebygge, etterforske, avsløre eller rettsforfølge straffbare forhold eller iverksette strafferettslige sanksjoner og om fri utveksling av slike opplysninger og om oppheving av rådsrammebeslutning 2008/977/JIS (EUT L 119 av 4.5.2016, s. 89).

(2) Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

(23) Det bør være tillatt å søke på fingeravtrykksopplysninger i SIS med fullstendige eller ufullstendige sett av fingeravtrykk eller håndflateavtrykk som er funnet på et åsted dersom det med stor sannsynlighet kan fastslås at de tilhører gjerningspersonen bak det alvorlige straffbare forholdet eller terrorhandlingen, forutsatt at et søk utføres samtidig i de relevante nasjonale fingeravtrykksdatabasene. Det bør legges særlig vekt på å fastsette kvalitetsstandarder for lagring av biometriske opplysninger.

(24) Dersom en persons identitet ikke kan fastslås på annen måte, bør fingeravtrykksopplysninger brukes for å forsøke å identifisere personen. Det bør i alle tilfeller være tillatt å identifisere en person ved hjelp av fingeravtrykksopplysninger.

(25) Medlemsstatene bør kunne kople sammen meldinger i SIS. Dersom to eller flere meldinger koples sammen, bør ikke det berøre tiltakene som skal treffes, undersøkelsesfristen for meldinger eller tilgangsrettighetene til meldingene.

(26) Det kan oppnås økt effektivitet, harmonisering og sammenheng ved å gjøre det obligatorisk å registrere i SIS alle innreiseforbud som nasjonale vedkommende myndigheter utsteder i samsvar med framgangsmåter som overholder

europaparlaments- og rådsdirektiv 2008/115/EF ([1]), og ved å fastsette felles regler for registrering av meldinger om nektet innreise og opphold ved tilbakesending av en tredjestatsborger med ulovlig opphold. Medlemsstatene bør treffe alle nødvendige tiltak for å sikre at det ikke er noe tidsintervall mellom tidspunktet tredjestatsborgeren forlater Schengen-området, og tidspunktet meldingen i SIS aktiveres. Dette bør sikre at innreiseforbud håndheves ved grenseoverganger ved de ytre grensene, og effektivt hindre fornyet innreise i Schengen-området.

(27) Personer som er gjenstand for beslutning om nektet innreise og opphold, bør ha adgang til å påklage denne beslutningen. Klageadgangen bør overholde direktiv 2008/115/EF dersom beslutningen er knyttet til tilbakesending.

(28) I denne forordning bør det fastsettes ufravikelige regler for samråd med og underretning av nasjonale myndigheter dersom en tredjestatsborger innehar eller kan skaffe en gyldig oppholdstillatelse eller et gyldig visum for langvarig opphold som er utstedt i én medlemsstat, og en annen medlemsstat planlegger å registrere eller allerede har registrert en melding om nektet innreise og opphold for den berørte tredjestatsborgeren. Slike situasjoner skaper stor usikkerhet for grensevakter, politi og innvandringsmyndigheter. Derfor bør det fastsettes en obligatorisk frist for samråd som raskt fører til et endelig resultat og sikrer at tredjestatsborgere som har rett til å ta lovlig opphold på medlemsstatenes territorium, kan reise inn på territoriet uten vanskeligheter, og at personer som ikke har rett til å reise inn, hindres i å gjøre det.

(29) Når en melding slettes i SIS etter samråd mellom medlemsstater, bør den innmeldende medlemsstaten kunne beholde den berørte tredjestatsborgeren på sin nasjonale meldingsliste.

(30) Denne forordning bør ikke berøre anvendelsen av europaparlaments- og rådsdirektiv 2004/38/EF ([2]).

(31) Meldinger bør ikke lagres i SIS lenger enn det som er nødvendig for å nå det særlige formålet som ligger til grunn for registreringen. Innen tre år etter at en melding er registrert i SIS, bør den innmeldende medlemsstaten undersøke om det er behov for fortsatt lagring. Dersom det i den nasjonale beslutning som ligger til grunn for meldingen, fastsettes en lengre gyldighetsperiode enn tre år, bør meldingen undersøkes innen fem år. Beslutninger om lagring av meldinger om personer bør bygge på en omfattende individuell vurdering. Medlemsstatene bør undersøke meldinger om personer innen den fastsatte undersøkelsesfristen og føre statistikk over antallet meldinger om personer der lagringstiden er forlenget.

(32) Registrering av en melding i SIS og forlengelse av utløpsdatoen for en melding i SIS bør være underlagt et krav til forholdsmessighet, herunder undersøkelse av om en konkret sak er adekvat, relevant og viktig nok til at en melding bør registreres i SIS. Når det gjelder terrorhandlinger, bør saken anses for å være adekvat, relevant og viktig nok til at en melding bør registreres i SIS. Av hensyn til den offentlige eller nasjonale sikkerhet bør medlemsstatene unntaksvis kunne unnlate å registrere en melding i SIS når det er sannsynlig at dette kan hindre offisielle eller rettslige undersøkelser, etterforskninger eller framgangsmåter.

(1) Europaparlaments- og rådsdirektiv 2008/115/EF av 16. desember 2008 om felles standarder og framgangsmåter i medlemsstatene for tilbakesending av tredjestatsborgere med ulovlig opphold (EUT L 348 av 24.12.2008, s. 98).

(2) Europaparlaments- og rådsdirektiv 2004/38/EF av 29. april 2004 om unionsborgeres og deres familiemedlemmers rett til å ferdes og oppholde seg fritt på medlemsstatenes territorium, om endring av forordning (EØF) nr. 1612/68 og om oppheving av direktiv 64/221/EØF, 68/360/EØF, 72/194/EØF, 73/148/EØF, 75/34/EØF, 75/35/EØF, 90/364/EØF, 90/365/EØF og 93/96/EØF (EUT L 158 av 30.4.2004, s. 77).

(33) SIS-opplysningenes integritet er av aller største betydning. Derfor bør det treffes nødvendige vernetiltak for behandling av SIS-opplysninger på sentralt og nasjonalt plan for å sikre at opplysningene er gjennomgående sikre. Myndigheter som behandler opplysninger, bør omfattes av sikkerhetskravene i denne forordning og en ensartet framgangsmåte for melding av hendelser. Personalet bør ha tilstrekkelig opplæring og underrettes om relevante straffbare forhold og strafferettslige sanksjoner.

(34) Opplysninger som behandles i SIS, og tilknyttede utfyllende opplysninger som utveksles i henhold til denne forordning, bør ikke overføres eller stilles til rådighet for tredjestater eller internasjonale organisasjoner.

(35) For å effektivisere innvandringsmyndighetenes arbeid når de skal treffe beslutninger om tredjestatsborgeres rett til innreise og opphold på medlemsstatenes territorium og om tilbakesending av tredjestatsborgere med ulovlig opphold, bør disse myndighetene gis tilgang til SIS i henhold til denne forordning.

(36) Uten at det berører nærmere regler for behandling av personopplysninger i denne forordning, bør forordning (EU) 2016/679 få anvendelse på medlemsstatenes behandling av personopplysninger i henhold til denne forordning, med mindre behandlingen utføres av nasjonale vedkommende myndigheter for å forebygge, etterforske, avsløre eller rettsforfølge terrorhandlinger eller andre alvorlige straffbare forhold.

(37) Uten at det berører nærmere regler i denne forordning, bør de nasjonale lovene og forskriftene vedtatt i henhold til direktiv (EU) 2016/680 få anvendelse på nasjonale vedkommende myndigheters behandling av personopplysninger i henhold til denne forordning for å forebygge, avsløre, etterforske eller rettsforfølge terrorhandlinger eller andre alvorlige straffbare

forhold eller fullbyrde strafferettslige sanksjoner. Tilgang til opplysninger som registreres i SIS, og rett til å søke i disse opplysningene for nasjonale vedkommende myndigheter med ansvar for å forebygge, avsløre, etterforske eller rettsforfølge terrorhandlinger eller andre alvorlige straffbare forhold eller for å fullbyrde strafferettslige sanksjoner må omfattes av alle relevant bestemmelser i denne forordning og i direktiv (EU) 2016/680 som innarbeidet i nasjonal rett, særlig tilsyn ført av tilsynsmyndighetene nevnt i direktiv (EU) 2016/680.

(38) Europaparlaments- og rådsforordning (EU) 2018/1725 ([1]) bør få anvendelse på unionsinstitusjonenes og -organenes behandling av personopplysninger når de ivaretar sine oppgaver i henhold til denne forordning.

(39) Europaparlaments- og rådsforordning (EU) 2016/794 ([2]) bør få anvendelse på Europols behandling av personopplysninger i henhold til denne forordning.

(40) Ved anvendelsen av SIS bør vedkommende myndigheter sikre at verdigheten og integriteten til den personen hvis opplysninger behandles, respekteres. Behandling av personopplysninger i henhold til denne forordning må ikke føre til forskjellsbehandling av personer på grunnlag av kjønn, rase eller etnisk opprinnelse, religion eller tro, funksjonshemming, alder eller seksuell legning.

(41) Når det gjelder fortrolighet, bør relevante bestemmelser i vedtektene for Den europeiske unions tjenestemenn og ansettelsesvilkårene for øvrige ansatte i Den europeiske union, fastsatt i rådsforordning (EØF, Euratom, EKSF) nr. 259/68 ([3]) («personalvedtektene»), få anvendelse på tjenestemenn og andre ansatte som arbeider med SIS.

(42) Både medlemsstatene og eu-LISA bør ha sikkerhetsplaner for å lette gjennomføringen av sikkerhetsforpliktelsene og bør samarbeide med hverandre slik at de behandler sikkerhetsspørsmål fra et felles perspektiv.

(43) De nasjonale uavhengige tilsynsmyndighetene nevnt i forordning (EU) 2016/679 og direktiv (EU) 2016/680 («tilsynsmyndighetene») bør overvåke at medlemsstatenes behandling av personopplysninger i henhold til denne forordning, herunder utveksling av utfyllende opplysninger, skjer på lovlig måte. Tilsynsmyndighetene bør gis tilstrekkelige ressurser til å utføre denne oppgaven. De registrertes rett til innsyn, retting og sletting av sine personopplysninger som er lagret i SIS, og eventuell etterfølgende klageadgang ved nasjonale domstoler samt gjensidig anerkjennelse av dommer, bør fastsettes. Det bør også kreves årlig statistikk fra medlemsstatene.

([1]) Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger og om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

(2) Europaparlaments- og rådsforordning (EU) 2016/794 av 11. mai 2016 om Den europeiske unions byrå for politisamarbeid (Europol) og erstatning og oppheving av rådsbeslutning 2009/371/JIS, 2009/934/JIS, 2009/935/JIS, 2009/936/JIS og 2009/968/JIS (EUT L 135 av 24.5.2016, s. 53)

(3) EFT L 56 av 4.3.1968, s. 1.

(44) Tilsynsmyndighetene bør sikre at det minst hvert fjerde år gjennomføres en revisjon av behandlingen av opplysninger i medlemsstatens nasjonale systemer i samsvar med internasjonale revisjonsstandarder. Revisjonen bør enten utføres av tilsynsmyndighetene, eller tilsynsmyndighetene bør bestille revisjonen direkte hos en uavhengig revisor med ekspertise innenfor personvern. Den uavhengige revisoren bør forbli under de berørte tilsynsmyndighetenes kontroll og ansvar, og disse bør derfor selv instruere revisoren og angi et klart definert formål og omfang og en klart definert metode for revisjonen samt veiledning og tilsyn med revisjonen og dens endelige resultater.

(45) EUs datatilsyn bør overvåke unionsinstitusjonenes og organenes virksomhett i forbindelse med behandling av personopplysninger i henhold til denne forordning. EUs datatilsyn bør samarbeide med tilsynsmyndighetene om tilsynet med SIS.

(46) EUs datatilsyn bør gis tilstrekkelige ressurser til å kunne utføre de oppgaver det er pålagt i henhold til denne forordning, herunder bistand fra personer med ekspertise innenfor biometriske opplysninger.

(47) I forordning (EU) 2016/794 fastsettes det at Europol skal støtte og styrke nasjonale vedkommende myndigheters innsats og deres samarbeid for å bekjempe terrorisme og grov kriminalitet, og utarbeide analyser og trusselvurderinger. For å gjøre det lettere for Europol å utføre sine oppgaver, særlig innenfor Det europeiske senter for migrantsmugling, bør Europol gis tilgang til meldingskategorier fastsatt i denne forordning.

(48) For å tette hullene med hensyn til deling av opplysninger om terrorisme, særlig om utenlandske fremmedkrigere dersom overvåking av deres bevegelser er avgjørende, oppfordres medlemsstatene til å dele opplysninger om terrorismerelatert aktivitet med Europol. Denne delingen av opplysninger bør skje ved at utfyllende opplysninger utveksles med Europol om de berørte meldingene. For dette formål bør Europol opprette en forbindelse med kommunikasjonsinfrastrukturen.

(49) Det er dessuten nødvendig å fastsette klare regler for Europol for behandling og nedlasting av SIS-opplysninger for å muliggjøre omfattende bruk av SIS, forutsatt at personvernstandardene i denne forordning og forordning (EU) 2016/794 overholdes. Dersom Europols søk i SIS viser at det finnes en melding registrert av en medlemsstat, kan ikke Europol treffe nødvendige tiltak. Europol bør derfor underrette den berørte medlemsstaten via utveksling av utfyllende opplysninger med det respektive SIRENE-kontor, slik at medlemsstaten kan følge opp saken.

(50) I henhold til europaparlaments- og rådsforordning (EU) 2016/1624 ([1]) skal vertsmedlemsstaten ved anvendelse av nevnte forordning tillate medlemmene i enhetene som er omhandlet i artikkel 2 nr. 8 i nevnte forordning, og som er utplassert av Det europeiske grense- og kystvaktbyrå, å foreta de søk i unionsdatabaser som er nødvendige for å oppfylle driftsmål angitt i driftsplanen for inn- og utreisekontroller, grenseovervåking og tilbakesending. Andre relevante EU-byråer, særlig Det europeiske asylstøttekontor og Europol, kan også utplassere eksperter som ikke er ansatt ved disse EU-byråene som en del av støttegruppene for migrasjonsstyring. Målet med innsetting av enhetene nevnt i artikkel 2 nr. 8 og 9 i nevnte forordning er å gi de medlemsstater som anmoder om det, teknisk og operativ støtte, særlig de medlemsstater som står overfor uforholdsmessig store migrasjonsutfordringer. For at enhetene omhandlet i artikkel 2 nr. 8 og 9 i nevnte forordning kan utføre sine oppgaver, har de bruk for tilgang til SIS via et teknisk grensesnitt hos Det europeiske grense- og kystvaktbyrå med forbindelse til det sentrale SIS. Dersom søk i SIS som enhetene nevnt i artikkel 2 nr. 8 og 9 i forordning (EU) 2016/1624 eller personalet foretar, viser at det finnes en melding registrert av en medlemsstat, kan ikke medlemmet i enheten eller personalet treffe nødvendige tiltak uten tillatelse fra vertsmedlemsstaten. Derfor bør vertsmedlemsstaten underrettes, slik at den kan følge opp saken. Vertsmedlemsstaten bør underrette den innmeldende medlemsstat om treffet via utveksling av utfyllende opplysninger.

(51) Visse aspekter ved SIS kan ikke dekkes uttømmende av denne forordning på grunn av deres tekniske, svært detaljerte og hyppig skiftende art. Disse aspektene omfatter for eksempel tekniske regler for registrering av, ajourføring av, sletting av og søk i opplysninger, datakvalitet og regler for biometriske opplysninger, regler om meldingers forenlighet og prioriteringsrekkefølge, koplinger mellom meldinger og utveksling av utfyllende opplysninger. Kommisjonen bør derfor gis gjennomføringsmyndighet for disse aspektene. Tekniske regler for søk i meldinger bør ta hensyn til at de nasjonale anvendelsene skal fungere effektivt.

([1]) Europaparlaments- og rådsforordning (EU) 2016/1624 av 14. september 2016 om den europeiske grense- og kystvakt og om endring av europaparlaments- og rådsforordning (EU) 2016/399 og om oppheving av europaparlaments- og rådsforordning (EF) nr. 863/2007, rådsforordning (EF) nr. 2007/2004 og rådsvedtak 2005/267/EF (EUT L 251 av 16.9.2016, s. 1).

(52) For å sikre ensartede vilkår for gjennomføringen av denne forordning bør Kommisjonen gis gjennomføringsmyndighet. Denne myndigheten bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011 ([1]). Framgangsmåten for vedtakelse av gjennomføringsrettsakter i henhold til denne forordning og forordning (EU) 2018/1862 bør være identisk.

(53) For å sikre åpenhet bør eu-LISA to år etter idriftsetting av SIS i henhold til denne forordning utarbeide en rapport om hvordan det sentrale SIS og kommunikasjonsinfrastrukturen fungerer teknisk, herunder sikkerheten i disse, og om bilateral og multilateral utveksling av utfyllende opplysninger. Kommisjonen bør framlegge en samlet evaluering hvert fjerde år.

(54) For å sikre at SIS fungerer effektivt, bør myndigheten til å vedta rettsakter delegeres til Kommisjonen i samsvar med artikkel 290 i TEUV med hensyn til fastsettelse av hvilke omstendigheter fotografier og ansiktsbilder kan brukes under for identifisering av personer i andre sammenhenger enn ved alminnelige grenseoverganger. Det er særlig viktig at Kommisjonen holder hensiktsmessige samråd under sitt forberedende arbeid, herunder på ekspertnivå, og at disse samrådene holdes i samsvar med prinsippene i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming ([2]). For å sikre lik deltakelse i forberedelsen av delegerte rettsakter mottar Europaparlamentet og Rådet alle dokumenter samtidig som medlemsstatenes eksperter, og deres eksperter har systematisk tilgang til møter i Kommisjonens ekspertgrupper som arbeider med forberedelse av delegerte rettsakter.

(55) Ettersom målene med denne forordning, dvs. å opprette og regulere et informasjonssystem i Unionen og utveksle tilknyttede ufyllende opplysninger, ikke i tilstrekkelig grad kan oppnås av medlemsstatene, men på grunn av deres art bedre kan oppnås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet i artikkel 5 i traktaten om Den europeiske union (TEU). I samsvar med forholdsmessighetsprinsippet i nevnte artikkel går denne forordning ikke lenger enn det som er nødvendig for å oppnå disse målene.

(56) Denne forordning er forenlig med de grunnleggende rettigheter og prinsippene som er anerkjent særlig i Den europeiske unions pakt om de grunnleggende rettigheter. Denne forordning er særlig i alle deler forenlig med vernet av personopplysninger i samsvar med artikkel 8 i Den europeiske unions pakt om grunnleggende rettigheter og forsøker samtidig å sørge for et sikkert miljø for alle personer som er bosatt på Unionens territorium, og beskyttelse for irregulære migranter mot utnyttelse og menneskehandel. I saker om barn bør barnets interesse være et primært hensyn.

(57) De anslåtte kostnadene ved oppgraderingen av nasjonale systemer og gjennomføringen av nye funksjoner forutsatt i denne forordning er lavere enn det resterende beløp i budsjettposten for intelligente grenser i europaparlaments- og rådsforordning (EU) nr. 515/2014 ([3]). Derfor bør midlene som er satt av til å utvikle IT-systemer som støtte for forvaltningen av migrasjonsstrømmer over de ytre grensene i henhold til forordning (EU) nr. 515/2014, tildeles medlemsstatene og eu-LISA. De finansielle kostnadene ved oppgraderingen av SIS og gjennomføringen av denne forordning bør overvåkes. Dersom de anslåtte kostnadene er høyere, bør det stilles unionsmidler til rådighet for å støtte medlemsstatene i samsvar med den relevante flerårlige finansielle rammen.

(58) I samsvar med artikkel 1 og 2 i protokoll nr. 22 om Danmarks holdning vedlagt TEU og TEUV deltar Danmark ikke i vedtakelsen av denne forordning, som ikke er bindende for og ikke får anvendelse i Danmark. Ettersom denne forordning er en utvikling av Schengen-regelverket, skal Danmark, i samsvar med artikkel 4 i protokollen, innen seks måneder etter at Rådet har truffet beslutning om denne forordning, beslutte om landet skal gjennomføre denne forordning i sin nasjonale rett.

([1]) Europaparlaments- og rådsforordning (EU) nr. 182/2011 av 16. februar 2011 om fastsettelse av allmenne regler og prinsipper for medlemsstatenes kontroll med Kommisjonens utøvelse av sin gjennomføringsmyndighet (EUT L 55 av 28.2.2011, s. 13).

([2]) EUT L 123 av 12.5.2016, s. 1.

(3) Europaparlaments- og rådsforordning (EU) nr. 515/2014 av 16. april 2014 om opprettelse av ordningen for økonomisk støtte til yttergrensene og visum som en del av fondet for indre sikkerhet, og om oppheving av beslutning nr. 574/2007/EF (EUT L 150 av 20.5.2014, s. 143).

(59) Denne forordning utgjør en utvikling av de bestemmelser i Schengen-regelverket som Det forente kongerike ikke deltar i etter rådsbeslutning 2000/365/EF ([1]); Det forente kongerike deltar derfor ikke i vedtakelsen av denne forordning, som ikke er bindende for og ikke får anvendelse i Det forente kongerike.

(60) Denne forordning utgjør en utvikling av de bestemmelser i Schengen-regelverket som Irland ikke deltar i etter rådsbeslutning 2002/192/EF ([2]); Irland deltar derfor ikke i vedtakelsen av denne forordning, som ikke er bindende for og ikke får anvendelse i Irland.

(61) Når det gjelder Island og Norge, utgjør denne forordning, i henhold til avtalen mellom Rådet for Den europeiske union og Republikken Island og Kongeriket Norge om disse to statenes tilknytning til gjennomføringen, anvendelsen og utviklingen av Schengen-regelverket, en utvikling av de bestemmelser i Schengen-regelverket ([3]) som er omfattet av området nevnt i artikkel 1 bokstav G) i rådsbeslutning 1999/437/EF ([4]).

(62) Når det gjelder Sveits, utgjør denne forordning, i henhold til avtalen mellom Den europeiske union, Det europeiske fellesskap og Det sveitsiske edsforbund om Det sveitsiske edsforbunds tilknytning til gjennomføringen, anvendelsen og utviklingen av Schengen-regelverket ([5]), en utvikling av de bestemmelser i Schengen-regelverket som er omfattet av området nevnt i artikkel 1 bokstav G) i beslutning 1999/437/EF sammenlignet med artikkel 3 i rådsbeslutning 2008/146/EF ([6]).

(63) Når det gjelder Liechtenstein, utgjør denne forordning, i henhold til protokollen mellom Den europeiske union, Det europeiske fellesskap, Det sveitsiske edsforbund og Fyrstedømmet Liechtenstein om Fyrstedømmet Liechtensteins tiltredelse til avtalen mellom Den europeiske union, Det europeiske fellesskap og Det sveitsiske edsforbund om Det sveitsiske edsforbunds tilknytning til gjennomføringen, anvendelsen og utviklingen av Schengen-regelverket, en utvikling av de bestemmelser i Schengen-regelverket ([7]) som er omfattet av området nevnt i artikkel 1 bokstav G) i beslutning 1999/437/EF sammenlignet med artikkel 3 i rådsbeslutning 2011/350/EU ([8]).

(64) Når det gjelder Bulgaria og Romania, utgjør denne forordning en rettsakt som bygger på eller på annen måte har tilknytning til Schengen-regelverket i henhold til artikkel 4 nr. 2 i tiltredelsesakten av 2005, og bør leses i sammenheng med rådsbeslutning 2010/365/EU ([9]) og (EU) 2018/934 ([10]).

(65) Når det gjelder Kroatia, utgjør denne forordning en rettsakt som bygger på eller på annen måte har tilknytning til Schengen-regelverket i henhold til artikkel 4 nr. 2 i tiltredelsesakten av 2011, og bør leses i sammenheng med rådsbeslutning (EU) 2017/733 ([11]).

(66) Når det gjelder Kypros, utgjør denne beslutning en rettsakt som bygger på eller på annen måte har tilknytning til Schengen-regelverket i henhold til artikkel 3 nr. 2 i tiltredelsesakten av 2003.

(67) Ved denne forordning innføres en rekke forbedringer av SIS som vil øke effektiviteten, styrke personvernet og utvide tilgangsrettighetene. Noen av disse forbedringene krever ikke kompleks teknisk utvikling, mens andre faktisk krever tekniske endringer av forskjellig størrelsesorden. For å gjøre det mulig å stille forbedringer av systemet til rådighet for sluttbrukerne så snart som mulig innføres det med denne forordning endringer i

([1]) Rådsbeslutning 2000/365/EF av 29. mai 2000 om anmodning fra Det forente kongerike Storbritannia og Nord-Irland om å delta i visse bestemmelser i Schengen-regelverket (EFT L 131 av 1.6.2000, s. 43).

([2]) Rådsbeslutning 2002/192/EF av 28. februar 2002 om anmodning fra Irland om å delta i visse bestemmelser i Schengen-regelverket (EUT L 64 av 7.3.2002, s. 20).

(3) EFT L 176 av 10.7.1999, s. 36.
(4) Rådsbeslutning 1999/437/EF av 17. mai 1999 om visse gjennomføringsbestemmelser til den avtale som Rådet for Den europeiske union har inngått med Republikken Island og Kongeriket Norge om disse to staters tilknytning til gjennomføringen, anvendelsen og utviklingen av Schengen-regelverket (EUT L 176 av 10.7.1999, s. 31).
(5) EUT L 53 av 27.2.2008, s. 52.
(6) Rådsbeslutning 2008/146/EF av 28. januar 2008 om inngåelse, på Det europeiske fellesskaps vegne, av avtalen mellom Den europeiske union, Det europeiske fellesskap og Det sveitsiske edsforbund om Det sveitsiske edsforbunds tilknytning til gjennomføringen, anvendelsen og utviklingen av Schengen-regelverket (EUT L 53 av 27.2.2008, s. 1).
(7) EUT L 160 av 18.6.2011, s. 21.
(8) Rådsbeslutning 2011/350/EU av 7. mars 2011 om inngåelse, på Den europeiske unions vegne, av protokollen mellem Den europeiske union, Det europeiske fellesskap, Det sveitsiske edsforbund og Fyrstedømmet Liechtenstein om Fyrstedømmet Liechtensteins tiltredelse til avtalen mellom Den europeiske union, Det europeiske fellesskap og Det sveitsiske edsforbund om Det sveitsiske edsforbunds tilknytning til gjennomføringen, anvendelsen og utviklingen av Schengen-regelverket, når det gjelder avskaffelse av kontroller ved de indre grenser og bevegelse av personer (EUT L 160 av 18.6.2011, s. 19).
(9) Rådsbeslutning 2010/365/EU av 29. juni 2010 om anvendelse av bestemmelsene i Schengen-regelverket om Schengen-informasjonssystemet i Republikken Bulgaria og Romania (EUT L 166 av 1.7.2010, s. 17).
(10) Rådsbeslutning (EU) 2018/934 av 25. juni 2018 om anvendelse av de resterende bestemmelser i Schengen-regelverket om Schengen-informasjonssystemet i Republikken Bulgaria og Romania (EUT L 165 av 2.7.2018, s. 37).
(11) Rådsbeslutning (EU) 2017/733 av 25. april 2017 om anvendelse av bestemmelsene i Schengen-regelverket om Schengen-informasjonssystemet i Republikken Kroatia (EUT L 108 av 26.4.2017, s. 31**).**

forordning (EF) nr. 1987/2006 i flere faser. En rekke forbedringer av systemet bør få anvendelse umiddelbart etter at denne forordning er trådt i kraft, mens andre bør få anvendelse enten ett eller to år etter at den har trådt i kraft. Denne forordning bør få anvendelse i alle deler innen tre år etter at den har trådt i kraft. For å unngå at anvendelsen forsinkes, bør den trinnvise gjennomføring av denne forordning overvåkes nøye.

(68) Forordning (EF) nr. 1987/2006 bør oppheves med virkning fra den dato denne forordning får anvendelse i sin helhet.

(69) EUs datatilsyn er blitt rådspurt i samsvar med artikkel 28 nr. 2 i europaparlaments- og rådsforordning (EF) nr. 45/2001 ([1]) og har avgitt uttalelse 3. mai 2017 —

VEDTATT DENNE FORORDNING:

KAPITTEL I

ALMINNELIGE BESTEMMELSER

Artikkel 1

Generelt formål med SIS

Formålet med SIS skal være å sikre, ved hjelp av opplysninger formidlet via dette systemet, et høyt sikkerhetsnivå innenfor området frihet, sikkerhet og rettferdighet i Unionen, herunder opprettholde offentlig orden og offentlig sikkerhet og ivareta sikkerheten på medlemsstatenes territorium, og sikre anvendelse av bestemmelsene om fri bevegelighet for personer i tredje del avdeling V kapittel 2 i TEUV på deres territorium.

Artikkel 2

Formål

1. I denne forordning fastsettes vilkår og framgangsmåter for registrering og behandling i SIS av meldinger om tredjestatsborgere og for utveksling av utfyllende opplysninger og tilleggsopplysninger med sikte på nektet innreise og opphold på medlemsstatenes territorium.

2. I denne forordning fastsettes også bestemmelser om den tekniske strukturen for SIS, ansvarsområdene til medlemsstatene og Den europeiske unions byrå for driftsforvaltning av store IT-systemer innenfor området frihet, sikkerhet og rettferdighet (eu-LISA), om behandling av opplysninger, om berørte personers rettighetene og om erstatningsansvar.

Artikkel 3

Definisjoner

I denne forordning menes med

(1) «melding» et sett opplysninger som registreres i SIS, og som gjør det mulig for vedkommende myndigheter å identifisere en person med sikte på å treffe særlige tiltak,

(2) «utfyllende opplysninger» opplysninger som ikke utgjør del av meldingsopplysningene som er lagret i SIS, men som er forbundet med meldinger i SIS, og som skal utveksles via SIRENE-kontorene

(a) for at medlemsstatene skal kunne rådføre seg med eller underrette hverandre i forbindelse med at de registrerer en melding,

(b) for at egnede tiltak skal kunne treffes ved et treff,

(c) når nødvendige tiltak ikke kan treffes,

(d) når det er snakk om kvaliteten på opplysningene i SIS,

(e) når det er snakk om meldingenes forenlighet og prioritering,

(f) når det er snakk om tilgangsrettigheter,

(3) «tilleggsopplysninger» opplysninger som er lagret i SIS, og som er forbundet med meldinger i SIS som umiddelbart skal gjøres tilgjengelige for vedkommende myndigheter når en person det er registrert opplysninger om i SIS, blir funnet som resultat av søk i SIS,

([1]) Europaparlaments- og rådsforordning (EF) nr. 45/2001 av 18. desember 2000 om personvern i forbindelse med behandling av personopplysninger i Fellesskapets institusjoner og organer og om fri utveksling av slike opplysninger (EFT L 8 av 12.1.2001, s. 1).

(4) «tredjestatsborger» en person som ikke er unionsborger i henhold til artikkel 20 nr. 1 i TEUV, med unntak av personer som har rett til fri bevegelighet likestilt med unionsborgeres rett i henhold til en avtale mellom Unionen eller Unionen og dens medlemsstater på den ene side og en tredjestat på den annen side,

(5) «personopplysninger» personopplysninger som definert i artikkel 4 nr. 1 i forordning (EU) 2016/679,

(6) «behandling av personopplysninger» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, logging, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,

(7) «sammenfall» forekomsten av følgende trinn:

(a) en sluttbruker har foretatt et søk i SIS,

(b) dette søket har vist at en annen medlemsstat har registrert en melding i SIS, og

(c) opplysninger om meldingen i SIS samsvarer med søkeopplysningene,

(8) «treff» ethvert sammenfall som oppfyller følgende kriterier:

(a) det er blitt bekreftet av

i) sluttbrukeren, eller

ii) vedkommende myndighet i samsvar med nasjonale framgangsmåter, dersom det berørte sammenfall var basert på sammenligning av biometriske opplysninger,

og

(b) det kreves ytterligere tiltak,

(9) «innmeldende medlemsstat» medlemsstaten som har registrert meldingen i SIS,

(10) «utstedende medlemsstat» medlemsstaten som vurderer å utstede eller forlenge, eller som har utstedt eller forlenget en oppholdstillatelse eller et visum for langvarig opphold, og som deltar i samrådsordningen med en annen medlemsstat,

(11) «fullbyrdende medlemsstat» medlemsstaten som treffer eller har truffet nødvendige tiltak etter et treff,

(12) «sluttbruker» en ansatt hos en vedkommende myndighet som har tillatelse til å søke direkte i CS-SIS, N.SIS eller en teknisk kopi,

(13) «biometriske opplysninger» personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske eller fysiologiske egenskaper, og som muliggjør eller bekrefter en entydig identifisering av nevnte fysiske person, f.eks. fotografier, ansiktsbilder og fingeravtrykksopplysninger,

(14) «fingeravtrykksopplysninger» opplysninger om fingeravtrykk og håndflateavtrykk som på grunn av sin unike art og referansepunktene i dem gjør det mulig å foreta nøyaktige og entydige sammenligninger for å fastslå en persons identitet,

(15) «ansiktsbilde» digitale bilder av ansiktet med tilstrekkelig bildeoppløsning og kvalitet til at de kan brukes til automatisk biometrisk sammenligning,

(16) «tilbakesending» tilbakesending som definert i artikkel 3 nr. 3 i direktiv 2008/115/EF,

(17) «innreiseforbud» et innreiseforbud som definert i artikkel 6 nr. 3 i direktiv 2008/115/EF,

(18) «terrorhandlinger» straffbare forhold i henhold til nasjonal rett nevnt i artikkel 3–14 i europaparlaments- og rådsdirektiv (EU) 2017/541 ([1]), eller tilsvarende et av disse straffbare forhold for medlemsstater som ikke er bundet av nevnte direktiv,

(19) «oppholdstillatelse» en oppholdstillatelse som definert i artikkel 2 nr. 16 i europaparlaments- og rådsforordning (EU) 2016/399 ([2]),

(20) «visum for langvarig opphold» et visum for langvarig opphold som nevnt i artikkel 18 nr. 1 i konvensjonen om gjennomføring av Schengen-avtalen,

(21) «trussel mot folkehelsen» en trussel mot folkehelsen som definert i artikkel 2 nr. 21 i forordning (EU) 2016/399.

([1]) Europaparlaments- og rådsdirektiv (EU) 2017/541 av 15. mars 2017 om bekjempelse av terrorisme og om erstatning av rådsrammebeslutning 2002/475/JIS og endring av rådsrammebeslutning 2005/671/JIS (EUT L 88 av 31.3.2017, s. 6).
([2]) Europaparlaments- og rådsforordning (EU) 2016/399 av 9. mars 2016 om et unionsregelverk som regulerer bevegelse av personer over grensene (Schengen-grenseregelverk) (EUT L 77 av 23.3.2016, s. 1).

Artikkel 4

Teknisk struktur og drift av SIS

1. SIS skal bestå av følgende deler:

(a) et sentralt system (det sentrale SIS) bestående av

i) en teknisk støttefunksjon («CS-SIS») som inneholder en database, («SIS-databasen»), herunder en reserve for CS-SIS, ii)

et ensartet nasjonalt grensesnitt («NI-SIS»),

(b) et nasjonalt system (N.SIS) i hver av medlemsstatene, bestående av et nasjonalt datasystem som kommuniserer med det sentrale SIS, herunder minst én nasjonal eller felles reserve for N.SIS, og

(c) en kommunikasjonsinfrastruktur mellom CS-SIS, en reserve for CS-SIS og NI-SIS («kommunikasjonsinfrastrukturen») med et kryptert virtuelt nettverk for SIS-opplysninger og utveksling av opplysninger mellom SIRENE-kontorene omhandlet i artikkel 7 nr. 2.

Et N.SIS som nevnt i bokstav b) kan inneholde en datafil («nasjonal kopi») som inneholder en fullstendig eller delvis kopi av SIS-databasen. To eller flere medlemsstater kan i et av sine N.SIS opprette en felles kopi som disse medlemsstatene kan bruke sammen. En slik felles kopi skal anses som hver av disse medlemsstatenes nasjonale kopi.

En felles reserve for N.SIS som nevnt i bokstav b) kan brukes sammen av to eller flere medlemsstater. I slike tilfeller skal den felles reserven for N.SIS anses som reserven for hver av disse medlemsstatenes reserve for N.SIS. N.SIS og dets reserve kan brukes samtidig for å sikre at systemet alltid er tilgjengelig for sluttbrukerne.

Medlemsstater som har til hensikt å opprette en felles kopi eller felles reserve for N.SIS som skal brukes sammen, skal enes om sine respektive ansvarsområder skriftlig. De skal underrette Kommisjonen om denne ordningen.

Kommunikasjonsinfrastrukturen skal støtte og bidra til å sikre at SIS alltid er tilgjengelig. Den skal omfatte redundante og atskilte søkeveier for forbindelsene mellom CS-SIS og reserven for CS-SIS og skal også omfatte redundante og atskilte søkeveier for forbindelsene mellom hvert nasjonalt SIS-nettilgangspunkt og CS-SIS og reserven for CS-SIS.

2. Medlemsstatene skal registrere, ajourføre, slette og søke i SIS-opplysninger via sitt eget N.SIS. Medlemsstater som bruker en delvis eller fullstendig nasjonal kopi eller en delvis eller fullstendig felles kopi, skal stille denne kopien til rådighet for elektroniske søk på territoriet til den enkelte medlemsstat. Den delvise nasjonale eller felles kopien skal inneholde minst opplysningene angitt i artikkel 20 nr. 2 bokstav a)–v). Det skal ikke være mulig å søke i datafilene i andre medlemsstaters N.SIS, unntatt ved felles kopier.

3. CS-SIS skal brukes til teknisk tilsyn og forvaltning og ha en reserve for CS-SIS, som skal kunne sikre alle funksjoner i CS-SIS-hovedsystemet dersom systemet skulle svikte. CS-SIS og reserven for CS-SIS skal plasseres i eu-LISAs to tekniske anlegg.

4. eu-LISA skal gjennomføre tekniske løsninger for å styrke den uavbrutte tilgangen til SIS enten via samtidig drift av CS-SIS og reserven for CS-SIS, forutsatt at reserven for CS-SIS fortsatt kan sikre driften av SIS dersom CS-SIS skulle svikte, eller via duplisering av systemet eller dets komponenter. Uten hensyn til saksbehandlingskravene fastsatt i artikkel 10 i forordning (EU) 2018/1726 skal eu-LISA senest 28. desember 2019 foreta en undersøkelse av mulige tekniske løsninger, som inneholder en uavhengig konsekvensvurdering og en nytte- og kostnadsanalyse.

5. Om nødvendig kan eu-LISA i unntakstilfeller midlertidig utvikle en ytterligere kopi av SIS-databasen.

6. CS-SIS skal levere tjenester som er nødvendige for å registrere og behandle opplysninger i SIS, herunder søke i SIS-databasen. For medlemsstater som bruker en nasjonal eller felles kopi, skal CS-SIS

(a) sørge for direktekoplede ajourføringer for de nasjonale kopiene,

(b) sikre synkronisering og sammenheng mellom de nasjonale kopiene og SIS-databasen, og

(c) utføre initialisering og gjenoppretting av nasjonale kopier.

7. CS-SIS skal sørge for uavbrutt tilgang.

Artikkel 5

Kostnader

1. Kostnadene ved drift, vedlikehold og videreutvikling av det sentrale SIS og kommunikasjonsinfrastrukturen skal dekkes over Unionens alminnelige budsjett. Disse kostnadene skal omfatte arbeid i forbindelse med CS-SIS for å sikre levering av tjenestene omhandlet i artikkel 4 nr. 6.

2. Det tildeles midler fra finansieringsrammen på 791 millioner euro fastsatt i artikkel 5 nr. 5 bokstav b) i forordning (EU) nr. 515/2014 for å dekke kostnadene ved gjennomføring av denne forordning.

3. Uten at det berører ytterligere midler for dette formål fra andre kilder i Unionens alminnelige budsjett, tildeles eu-LISA et beløp på 31 098 000 euro fra finansierinsrammen i nr. 2. Denne finansieringen skal gjennomføres ved indirekte forvaltning og skal bidra til å gjennomføre den tekniske utvikling som kreves i henhold til denne forordning når det gjelder det sentrale SIS og kommunikasjonsinfrastrukturen samt tilknyttede opplæringsaktiviteter.

4. Fra finansieringsrammen i nr. 2 skal medlemsstatene som deltar i forordning (EU) nr. 515/2014, motta en ekstra samlet bevilling på 36 810 000 euro som skal fordeles i like deler som et engangsbeløp til deres grunnbevilling. Denne finansieringen skal gjennomføres ved delt forvaltning og skal i sin helhet anvendes til rask og effektiv oppgradering av de berørte nasjonale systemer i samsvar med kravene i denne forordning.

5. Kostnadene ved opprettelse, drift, vedlikehold og videreutvikling av de enkelte N.SIS skal dekkes av vedkommende medlemsstat.

KAPITTEL II

MEDLEMSSTATENES ANSVAR

Artikkel 6

Nasjonale systemer

Hver medlemsstat skal ha ansvaret for å opprette, drifte, vedlikeholde og videreutvikle sitt eget N.SIS og knytte det til NI-SIS.

Hver medlemsstat skal ha ansvaret for å sikre uavbrutt tilgang til SIS-opplysninger for sluttbrukerne.

Hver medlemsstat skal overføre sine meldinger via sitt eget N.SIS.

Artikkel 7

N.SIS- og SIRENE-kontoret

1. Hver medlemsstat skal utpeke en myndighet (N.SIS-kontoret) som skal ha det sentrale ansvaret for N.SIS.

Denne myndigheten skal ha ansvaret for at N.SIS fungerer sikkert og effektivt, sikre vedkommende myndigheter tilgang til SIS og treffe nødvendige tiltak for å sikre at denne forordning overholdes. Myndigheten skal ha ansvaret for å sikre at alle funksjoner i SIS på hensiktsmessig måte stilles til rådighet for sluttbrukerne.

2. Hver medlemsstat skal utpeke en nasjonal myndighet (SIRENE-kontoret) som skal være i drift 24 timer i døgnet 7 dager i uken, og som skal sikre utveksling av og tilgang til alle utfyllende opplysninger i samsvar med SIRENE-håndboken. Hvert SIRENE-kontor skal være et enkelt kontaktpunkt for sin medlemsstat med sikte på å utveksle utfyllende opplysninger om meldinger og gjøre det lettere å treffe nødvendige tiltak når det er registrert meldinger om personer i SIS, og disse personene lokaliseres etter et treff.

Hvert SIRENE-kontor skal i samsvar med nasjonal rett ha enkel, direkte eller indirekte tilgang til alle relevante nasjonale opplysninger, herunder nasjonale databaser og alle opplysninger om sin medlemsstats egne meldinger, og til ekspertrådgivning for å kunne reagere på anmodninger om utfyllende opplysninger rask og innen fristene fastsatt i artikkel 8.

SIRENE-kontorene skal samordne kontrollen av kvaliteten på opplysningene som registreres i SIS. For disse formål skal de ha tilgang til opplysningene som behandles i SIS.

3. Medlemsstatene skal gi eu-LISA opplysninger om sitt N.SIS-kontor og sitt SIRENE-kontor. eu-LISA skal offentliggjøre en liste over N.SIS-kontorene og SIRENE-kontorene sammen med listen nevnt i artikkel 41 nr. 8.

Artikkel 8

Utveksling av utfyllende opplysninger

1. Utfyllende opplysninger skal utveksles i samsvar med SIRENE-håndboken via kommunikasjonsinfrastrukturen. Medlemsstatene skal sørge for nødvendige tekniske og menneskelige ressurser for å sikre uavbrutt tilgang til og rask og effektiv utveksling av utfyllende opplysninger. Dersom kommunikasjonsinfrastrukturen ikke er tilgjengelig, skal medlemsstatene bruke annen tilstrekkelig sikker teknikk til utveksling av utfyllende opplysninger. En liste over tilstrekkelig sikker teknikk skal fastsettes

i SIRENE-håndboken.

2. Utfyllende opplysninger skal brukes bare for det formål de ble overført i samsvar med artikkel 49, med mindre det er innhentet forutgående samtykke til annen bruk fra den innmeldende medlemsstaten.

3. SIRENE-kontorene skal utføre sine oppgaver rask og effektivt, særlig ved å svare på en anmodning om utfyllende opplysninger så snart som mulig og senest 12 timer etter at anmodningen er mottatt.

Anmodninger om utfyllende opplysninger med høyest prioritet skal merkes med påskriften «URGENT» i SIRENE-skjemaene og en begrunnelse for hvorfor saken haster.

4. Kommisjonen skal vedta gjennomføringsrettsakter for å fastsette nærmere regler for SIRENE-kontorenes oppgaver i henhold til denne forordning og utveksling av utfyllende opplysninger i form av en håndbok med tittelen «SIRENE-håndboken». Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

Artikkel 9

Teknisk og funksjonelt samsvar

1. For å sikre rask og effektiv overføring av opplysninger skal hver medlemsstat, ved opprettelsen av sitt eget N.SIS, overholde felles standarder, protokoller og tekniske framgangsmåter som er fastsatt for å sikre kompatibilitet mellom N.SIS og det sentrale SIS.

2. Dersom en medlemsstat bruker en nasjonal kopi, skal den ved hjelp av tjenestene fra CS-SIS og gjennom de automatiske oppdateringene omhandlet i artikkel 4 nr. 6 sikre at opplysninger som lagres i den nasjonale kopien, er identiske og i samsvar med opplysningene i SIS-databasen, og at søk i den nasjonale kopien gir samme resultater som søk i SIS-databasen.

3. Sluttbrukerne skal motta nødvendige opplysninger for å utføre sine oppgaver, særlig og ved behov alle tilgjengelige opplysninger som gjør det mulig å identifisere den registrerte og treffe nødvendige tiltak.

4. Medlemsstatene og eu-LISA skal foreta regelmessige utprøvinger for å kontrollere det tekniske samsvar ved de nasjonale kopiene nevnt i nr. 2. Det skal tas hensyn til disse utprøvingene som ledd i mekanismen opprettet ved rådsforordning (EU) nr. 1053/2013 ([1]).

5. Kommisjonen skal vedta gjennomføringsrettsakter for å fastsette og utvikle felles standarder, protokoller og tekniske framgangsmåter i henhold til nr. 1 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

Artikkel 10

Sikkerhet – medlemsstatene

1. Hver medlemsstat skal i forbindelse med sitt eget N.SIS treffe nødvendige tiltak, herunder utarbeide en sikkerhetsplan, en plan for kontinuerlig virksomhet og en katastrofeplan, for

(a) fysisk å beskytte opplysninger, herunder utarbeide beredskapsplaner for å beskytte kritisk infrastruktur,

(b) å hindre at uvedkommende får adgang til datainstallasjoner som brukes til behandling av personopplysninger (adgangskontroll),

(c) å hindre at uvedkommende leser, kopierer, endrer eller fjerner datamedier (kontroll av datamedier),

([1]) Rådsforordning (EU) nr. 1053/2013 av 7. oktober 2013 om opprettelse av en vurderings- og overvåkingsmekanisme for kontroll av anvendelsen av Schengen-regelverket og om oppheving av styringskomiteens avgjørelse av 16. september 1998 om nedsettelse av en fast komité for vurdering og gjennomføring av Schengen-regelverket (EUT L 295 av 6.11.2013, s. 27).

(d) å hindre at uvedkommende registrerer opplysninger, og at uvedkommende får innsyn i, endrer og sletter personopplysninger (kontroll av registrering),

(e) å hindre at uvedkommende bruker systemer for elektronisk behandling av opplysninger ved hjelp av dataoverføringsutstyr (kontroll av bruker),

(f) å hindre at uvedkommende behandler opplysninger i SIS, og at uvedkommende endrer eller sletter opplysninger som er behandlet i SIS (kontroll med registrering av opplysninger),

(g) å sikre at personer med tillatelse til å bruke et elektronisk system for behandling av opplysninger får tilgang bare til opplysninger omfattet av tillatelsen deres og bare ved hjelp av individuelle og unike brukeridentifikatorer og fortrolige tilgangsmetoder (tilgangskontroll),

(h) å sikre at alle myndigheter med tilgangsrett til SIS eller til datainstallasjonene oppretter profiler som beskriver funksjoner og

ansvarsområder for personer som har tillatelse til å lese, registrere, ajourføre, slette og søke i opplysninger og på anmodning uten opphold gjøre disse profilene tilgjengelige for tilsynsmyndighetene omhandlet i artikkel 55 nr. 1 (personalprofiler),

(i) å sikre at det er mulig å kontrollere og fastslå hvilke organer personopplysninger kan overføres til ved bruk av dataoverføringsutstyr (kommunikasjonskontroll),

(j) å sikre at det i etterkant er mulig å kontrollere og fastslå hvilke personopplysninger som er registrert i de elektroniske systemene for behandling av opplysninger, og når, av hvem og for hvilket formål (registreringskontroll),

(k) å hindre at uvedkommende leser, kopierer, endrer eller sletter personopplysninger under overføring av personopplysninger eller transport av datamedier, særlig ved hjelp av hensiktsmessige krypteringsteknikker (transportkontroll),

(l) å overvåke at sikkerhetstiltakene i dette nummer er effektive, og iverksette nødvendige organisatoriske tiltak for intern overvåking for å sikre at denne forordning overholdes (egenrevisjon),

(m) å sikre at de installerte systemene ved avbrudd kan gjenopprettes til normal drift (gjenoppretting), og

(n) å sikre at SIS fungerer tilfredsstillende, at feil rapporteres (pålitelighet), og at personopplysninger lagret i SIS ikke kan ødelegges ved hjelp av systemsvikt (integritet).

2. Medlemsstatene skal ved behandling og utveksling av utfyllende opplysninger treffe tiltak med hensyn til sikkerhet tilsvarende tiltakene nevnt i nr. 1, herunder sikre SIRENE-kontorenes lokaler.

3. Medlemsstatene skal ved myndighetenes behandling av SIS-opplysninger nevnt i artikkel 34 treffe tiltak med hensyn til sikkerhet tilsvarende tiltakene nevnt i nr. 1 i denne artikkel.

4. Tiltakene beskrevet i nr. 1, 2 og 3 kan være ledd i en alminnelig sikkerhetsstrategi og -plan på nasjonalt plan som omfatter flere IT-systemer. I slike tilfeller skal kravene i denne artikkel og deres anvendelse på SIS tydelig framgå av og sikres med denne planen.

Artikkel 11

Fortrolighet – medlemsstatene

1. Hver medlemsstat skal i samsvar med nasjonal rett anvende egne regler for taushetsplikt eller annen tilsvarende fortrolighetsplikt på alle personer og organer som arbeider med SIS-opplysninger og utfyllende opplysninger. Denne plikten skal også gjelde etter at disse personene har sluttet i sin stilling, ansettelsesforholdet er opphørt eller organets virksomhet er avsluttet.

2. Dersom en medlemsstat samarbeider med eksterne leverandører i forbindelse med SIS-relaterte oppgaver, skal den nøye overvåke leverandørens virksomhet for å sikre at alle bestemmelser i denne forordning overholdes, særlig med hensyn til sikkerhet, fortrolighet og personvern.

3. Driftsforvaltningen av N.SIS eller av tekniske kopier skal ikke overlates til private foretak eller private organisasjoner.

Artikkel 12

Føring av logger på nasjonalt plan

1. Medlemsstater skal sikre at enhver tilgang til og utveksling av personopplysninger i CS-SIS loggføres i N.SIS for å kontrollere om søket var lovlig, overvåke at behandlingen av opplysninger er lovlig, utføre egenkontroll, sikre at N.SIS fungerer tilfredsstillende, og garantere opplysningenes integritet og sikkerhet. Dette kravet gjelder ikke de automatiske prosessene i artikkel 4 nr. 6 bokstav a), b) og c).

2. Loggene skal særlig vise meldingshistorikk, dato og klokkeslett for behandling av opplysninger, hvilke opplysninger som er brukt til søket, en henvisning til behandlede opplysninger og de individuelle og unike brukeridentifikatorer både for vedkommende myndighet og personen som behandlet opplysningene.

3. Dersom et søk utføres med fingeravtrykksopplysninger eller ansiktsbilder i samsvar med artikkel 33, skal loggene som unntak fra nr. 2 i denne artikkel vise hvilken type opplysninger som er brukt til søket i stedet for de faktiske opplysningene.

4. Loggene skal brukes bare for formålet i nr. 1 og skal slettes tre år etter at de er opprettet. Logger som inneholder meldingshistorikk, skal slettes tre år etter at meldingene er slettet.

5. Logger kan lagres lenger enn periodene nevnt i nr. 4 dersom de trengs til overvåkingsprosedyrer som allerede pågår.

6. Nasjonale vedkommende myndigheter med ansvar for å kontrollere om søk er lovlige, overvåke at behandlingen av opplysninger skjer på lovlig måte, utføre egenkontroll, sikring at N.SIS fungerer tilfredsstillende, og garantere opplysningenes integritet og sikkerhet, skal innenfor rammen av sine fullmakter på anmodning ha tilgang til loggene for å kunne utføre sine plikter.

Artikkel 13

Egenkontroll

Medlemsstatene skal sikre at enhver myndighet som har tilgangsrett til SIS-opplysninger, treffer nødvendige tiltak for å overholde denne forordning og ved behov samarbeide med tilsynsmyndigheten.

Artikkel 14

Opplæring av personale

1. Personale hos myndigheter med tilgangsrett til SIS skal, før de får tillatelse til å behandle opplysninger som er lagret i SIS, og regelmessig etter at det er gitt tilgang til SIS-opplysninger, få egnet opplæring i datasikkerhet, grunnleggende rettigheter, herunder personvern, og reglene og framgangsmåtene for behandling av opplysninger i SIRENE-håndboken. Personalet skal underrettes om relevante bestemmelser om straffbare forhold og strafferettslige sanksjoner, herunder de som er fastsatt i artikkel 59.

2. Medlemsstatene skal ha et nasjonalt opplæringsprogram for SIS som skal omfatte opplæring for både sluttbrukere og SIRENE-kontorenes personale.

Opplæringsprogrammet kan være en del av et generelt opplæringsprogram på nasjonalt plan som omfatter opplæring på andre relevante områder.

3. Felles opplæring skal organiseres på unionsplan minst én gang i året for å styrke samarbeidet mellom SIRENE-kontorene.

KAPITTEL III

eu-LISAs ANSVAR

Artikkel 15

Driftsforvaltning

1. eu-LISA skal ha ansvaret for driftsforvaltningen av det sentrale SIS. eu-LISA skal i samarbeid med medlemsstatene sikre at beste tilgjengelige teknologi i henhold til en nytte- og kostnadsanalyse alltid brukes for det sentrale SIS.

2. eu-LISA skal også ha ansvaret for følgende oppgaver i forbindelse med kommunikasjonsinfrastrukturen:

(a) tilsyn,

(b) sikkerhet,

(c) samordning av forbindelsene mellom medlemsstatene og leverandøren,

(d) oppgaver i forbindelse med gjennomføring av budsjettet,

(e) anskaffelse og fornying, og

(f) kontraktsmessige forhold.

3. eu-LISA skal også ha ansvaret for følgende oppgaver i forbindelse med SIRENE-kontorene og kommunikasjonen mellom SIRENE-kontorene:

(a) samordning, forvaltning av og støtte til utprøvinger,

(b) opprettholdelse og ajourføring av tekniske spesifikasjoner for utveksling av utfyllende opplysninger mellom SIRENE-kontorene og kommunikasjonsinfrastrukturen, og

(c) håndtering av innvirkningen av tekniske endringer som påvirker både SIS og utveksling av utfyllende opplysninger mellom SIRENE-kontorene.

4. eu-LISA skal utvikle og opprettholde en mekanisme og framgangsmåter for kvalitetskontroller av opplysningene i CS-SIS. Det skal regelmessig framlegge rapporter for medlemsstatene i denne forbindelse.

eu-LISA skal regelmessig framlegge en rapport for Kommisjonen om problemer som har oppstått, og medlemsstater som er berørt.

Kommisjonen skal regelmessig framlegge en rapport for Europaparlamentet og Rådet om problemer som har oppstått med opplysningenes kvalitet.

5. eu-LISA skal også utføre oppgaver i forbindelse med opplæring i teknisk bruk av SIS og tiltak for å forbedre kvaliteten på

SIS-opplysningene.

6. Driftsforvaltningen av det sentrale SIS skal omfatte alle nødvendige oppgaver for at det sentrale SIS skal kunne fungere 24 timer i døgnet 7 dager i uken i henhold til denne forordning, særlig nødvendig vedlikehold og teknisk utveksling for at systemet skal kunne fungere effektivt. Disse oppgavene skal også omfatte samordning, forvaltning og støtte til utprøvinger for det sentrale SIS og N.SIS som sikrer at det sentrale SIS og N.SIS fungerer i samsvar med kravene til teknisk og funksjonelt samsvar fastsatt i artikkel 9.

7. Kommisjonen skal vedta gjennomføringsrettsakter for å fastsette tekniske krav til kommunikasjonsinfrastrukturen. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

Artikkel 16

Sikkerhet – eu-LISA

1. eu-LISA skal treffe nødvendige tiltak, herunder utarbeide en sikkerhetsplan, en plan for kontinuerlig virksomhet og en katastrofeplan for det sentrale SIS og kommunikasjonsinfrastrukturen, for

(a) fysisk å beskytte opplysninger, herunder utarbeide beredskapsplaner for å beskytte kritisk infrastruktur,

(b) å hindre at uvedkommende får adgang til datainstallasjoner som brukes til behandling av personopplysninger (adgangskontroll),

(c) å hindre at uvedkommende leser, kopierer, endrer eller fjerner datamedier (kontroll av datamedier),

(d) å hindre at uvedkommende registrerer opplysninger, og at uvedkommende får innsyn i, endrer og sletter personopplysninger (kontroll av registrering),

(e) å hindre at uvedkommende bruker systemer for elektronisk behandling av opplysninger ved hjelp av dataoverføringsutstyr (kontroll av bruker),

(f) å hindre at uvedkommende behandler opplysninger i SIS, og at uvedkommende endrer eller sletter opplysninger som er behandlet i SIS (kontroll med registrering av opplysninger),

(g) å sikre at personer med tillatelse til å bruke et elektronisk system for behandling av opplysninger får tilgang bare til opplysninger omfattet av tillatelsen deres og bare ved hjelp av individuelle og unike brukeridentifikatorer og fortrolige tilgangsmetoder (tilgangskontroll),

(h) å opprette profiler som beskriver funksjoner og ansvarsområder for personer med tilgangsrett til opplysningene eller datainstallasjonene og på anmodning og uten opphold gi EUs datatilsyn tilgang til disse profilene (personalprofiler),

(i) å sikre at det er mulig å kontrollere og fastslå hvilke organer personopplysninger kan overføres til ved bruk av dataoverføringsutstyr (kommunikasjonskontroll),

(j) å sikre at det i etterkant er mulig å kontrollere og fastslå hvilke personopplysninger som er registrert i de elektroniske systemene for behandling av opplysninger, og når, av hvem og for hvilket formål (registreringskontroll),

(k) å hindre at uvedkommende leser, kopierer, endrer eller sletter personopplysninger under overføring av personopplysninger eller transport av datamedier, særlig ved hjelp av hensiktsmessige krypteringsteknikker (transportkontroll),

(l) å overvåke at sikkerhetstiltakene i dette nummer er effektive, og iverksette nødvendige organisatoriske tiltak for intern overvåking for å sikre at denne forordning overholdes (egenrevisjon),

(m) å sikre at de installerte systemene ved driftsavbrudd kan gjenopprettes til normal drift (gjenoppretting),

(n) å sikre at SIS fungerer tilfredsstillende, at feil rapporteres (pålitelighet), og at personopplysninger lagret i SIS ikke kan ødelegges ved hjelp av systemsvikt (integritet), og

(o) å sikre at dets tekniske anlegg er sikre.

2. eu-LISA skal treffe tiltak tilsvarende tiltakene i nr. 1 med hensyn til sikkerheten ved behandling og utveksling av utfyllende opplysninger via kommunikasjonsinfrastrukturen.

Artikkel 17

Fortrolighet – eu-LISA

1. Uten at det berører artikkel 17 i personalvedtektene skal eu-LISA anvende hensiktsmessige regler for taushetsplikt eller annen tilsvarende fortrolighetsplikt som kan sammenlignes med det som er fastsatt i artikkel 11 i denne forordning, på alt personale som arbeider med SIS-opplysninger. Denne plikten skal også gjelde etter at disse personene har sluttet i sin stilling, ansettelsesforholdet er opphørt eller deres virksomhet er avsluttet.

2. eu-LISA skal treffe tiltak tilsvarende tiltakene i nr. 1 med hensyn til fortrolighet ved utveksling av utfyllende opplysninger

via kommunikasjonsinfrastrukturen.

3. Dersom eu-LISA samarbeider med eksterne leverandører i forbindelse med SIS-relaterte oppgaver, skal det nøye overvåke leverandørens virksomhet for å sikre at alle bestemmelser i denne forordning overholdes, særlig med hensyn til sikkerhet, fortrolighet og personvern.

4. Driftsforvaltningen av CS-SIS skal ikke overlates til private foretak eller private organisasjoner.

Artikkel 18

Føring av logger på sentralt plan

1. eu-LISA skal sikre at enhver tilgang til og utveksling av personopplysninger i CS-SIS loggføres for formålene angitt i artikkel 12 nr. 1.

2. Loggene skal særlig vise meldingshistorikk, dato og klokkeslett for behandling av opplysninger, hvilke opplysninger som er brukt til søket, en henvisning til behandlede opplysninger og de individuelle og unike brukeridentifikatorer for vedkommende myndighet som behandlet opplysningene.

3. Dersom et søk utføres med fingeravtrykksopplysninger eller ansiktsbilder i samsvar med artikkel 33, skal loggene som unntak fra nr. 2 i denne artikkel vise hvilken type opplysninger som er brukt til søket i stedet for de faktiske opplysningene.

4. Loggene skal brukes bare for formålene i nr. 1 og skal slettes tre år etter at de er opprettet. Logger som inneholder meldingshistorikk, skal slettes tre år etter at meldingene er slettet.

5. Logger kan lagres lenger enn periodene nevnt i nr. 4 dersom de trengs til overvåkingsprosedyrer som allerede pågår.

6. For å utføre egenkontroll, sikre at CS-SIS fungerer tilfredsstillende, og garantere opplysningenes integritet og sikkerhet, skal eu-LISA ha tilgang til loggene innenfor rammene for sine fullmakter.

EUs datatilsyn skal på anmodning ha tilgang til disse loggene innenfor rammene for sine fullmakter og for å utføre sine oppgaver.

KAPITTEL IV

INFORMASJON TIL OFFENTLIGHETEN

Artikkel 19

SIS-informasjonskampanjer

Når denne forordning begynner å komme til anvendelse, skal Kommisjonen i samarbeid med tilsynsmyndighetene og EUs datatilsyn gjennomføre en kampanje for å underrette offentligheten om formålene med SIS, hvilke opplysninger som lagres i SIS, hvilke myndigheter som har tilgang til SIS, og de registrertes rettigheter. Kommisjonen skal regelmessig gjenta slike kampanjer i samarbeid med tilynsmyndighetene og EUs datatilsyn. Kommisjonen skal drive et nettsted som er tilgjengelig for offentligheten og inneholder alle relevante opplysninger om SIS. Medlemsstatene skal, i samarbeid med tilsynsmyndighetene, utarbeide og gjennomføre nødvendige strategier for å gi sine borgere og beboere generelle opplysninger om SIS.

KAPITTEL V

MELDINGER OM NEKTET INNREISE OG OPPHOLD FOR TREDJESTATSBORGERE

Artikkel 20

Kategorier av opplysninger

1. Uten at det berører artikkel 8 nr. 1 eller bestemmelsene i denne forordning om lagring av utdypende opplysninger, skal SIS inneholde bare de kategorier av opplysninger som meldes inn av hver enkelt medlemsstat, og som kreves for formålene i artikkel 24 og 25.

2. En melding i SIS som inneholder opplysninger om personer, skal inneholde bare følgende:

(a) etternavn,

(b) fornavn,

(c) navn ved fødsel,

(d) tidligere brukte navn og aliasnavn,

(e) særlige objektive fysiske kjennetegn av uforanderlig art,

(f) fødested,

(g) fødselsdato,

(h) kjønn,

(i) samtlige nasjonaliteter,

(j) om den berørte personen

i) er bevæpnet,

(ii) er voldelig,

(iii) har forsvunnet eller rømt,

(iv) er suicidal,

(v) utgjør en fare for folkehelsen, eller

(vi) deltar i en aktivitet nevnt i artikkel 3–14 i direktiv (EU) 2017/541,

(k) begrunnelse for meldingen,

(l) myndighet som har opprettet meldingen,

(m) henvisning til beslutningen som ligger til grunn for meldingen,

(n) tiltak som skal treffes ved et treff,

(o) koplinger til andre meldinger i samsvar med artikkel 48,

(p) om vedkommende er familiemedlem av en unionsborger eller en annen person som har rett til fri bevegelighet i henhold til artikkel 26,

(q) om beslutningen om nektet innreise og opphold er basert på

i) en tidligere dom som nevnt i artikkel 24 nr. 2 bokstav a),

(ii) en alvorlig sikkerhetstrussel som nevnt i artikkel 24 nr. 2 bokstav b),

(iii) omgåelse av unionsretten eller nasjonal rett om innreise og opphold som nevnt i artikkel 24 nr. 2 bokstav c),

(iv) et innreiseforbud som nevnt i artikkel 24 nr. 1 bokstav b), eller

(v) et restriktivt tiltak som nevnt i artikkel 25,

(r) typen straffbart forhold,

(s) arten av personens identitetsdokumenter,

(t) land som har utstedt personens identitetsdokumenter,

(u) nummer/numre på personens identifitetsdokumenter,

(v) dato for utstedelse av personens identitetsdokumenter,

(w) fotografier og ansiktsbilder,

(x) fingeravtrykksopplysninger,

(y) en kopi av identitetsdokumentene, om mulig i farger.

3. Kommisjonen skal vedta gjennomføringsrettsakter for å fastsette og utvikle nødvendige tekniske regler for å registrere, ajourføre, slette og søke i opplysningene nevnt i nr. 2 i denne artikkel samt felles standarder nevnt i nr. 4 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

4. De tekniske reglene skal være enslydende for søk i CS-SIS, i nasjonale eller felles kopier og i tekniske kopier i henhold til artikkel 41 nr. 2. De skal bygge på felles standarder.

Artikkel 21

Forholdsmessighet

1. Før medlemsstatene registrerer en melding, og når de forlenger en meldings gyldighetsperiode, skal de undersøke om saken er adekvat, relevant og viktig nok til at en melding bør registreres i SIS.

2. Dersom beslutningen om nektet innreise og opphold nevnt i artikkel 24 nr. 1 bokstav a) er knyttet til en terrorhandling, skal saken anses for å være adekvat, relevant og viktig nok til at en melding bør registreres i SIS. Av hensyn til den offentlige eller nasjonale sikkerhet kan medlemsstatene unntaksvis unnlate å registrere en melding når det er sannsynlig at den vil hindre offisielle eller rettslige undersøkelser, etterforskninger eller framgangsmåter.

Artikkel 22

Krav til registrering av en melding

1. Nødvendige minsteopplysninger for å registrere en melding i SIS er opplysningene nevnt i artikkel 20 nr. 2 bokstav a), g), k), m), n) og q). De andre opplysningene omhandlet i nevnte nummer skal også registreres i SIS, dersom de er tilgjengelige.

2. Opplysningene nevnt i artikkel 20 nr. 2 bokstav e) i denne forordning skal registreres bare når dette er absolutt nødvendig for å identifisere den berørte tredjestatsborgeren. Når slike opplysninger registreres, skal medlemsstatene sikre at artikkel 9 i forordning (EU) 2016/679 overholdes.

Artikkel 23

Forenlighet mellom meldinger

1. Før en melding registreres, skal medlemsstaten kontrollere om det allerede finnes en melding i SIS om den aktuelle personen. For det formål foretas det også en kontroll med fingeravtrykksopplysninger dersom slike opplysninger er tilgjengelige.

2. Det skal registreres bare én melding i SIS per person per medlemsstat. Dersom det er nødvendig, kan nye meldinger om samme person registreres av andre medlemsstater i samsvar med nr. 3.

3. Når det allerede finnes en melding i SIS om en bestemt person, skal medlemsstaten som ønsker å registrere en ny melding, kontrollere at meldingene er forenlige. Dersom de er forenlige, kan medlemsstaten registrere den nye meldingen. Dersom meldingene er uforenlige, skal de berørte medlemsstatenes SIRENE-kontorer rådføre seg med hverandre via utveksling av utfyllende opplysninger for å nå fram til en avtale. Reglene for forenlighet mellom meldinger skal fastsettes i SIRENE-håndboken. Reglene for forenlighet kan fravikes etter samråd mellom medlemsstatene dersom viktige nasjonale interesser står på spill.

4. Ved treff på flere meldinger om samme person skal den fullbyrdende medlemsstaten overholde prioriteringsrekkefølgen for meldinger i henhold til SIRENE-håndboken.

Dersom en person er omfattet av flere meldinger registrert av forskjellige medlemsstater, skal meldinger om pågripelse som er registrert i samsvar med artikkel 26 i forordning (EU) 2018/1862, fullbyrdes først, med forbehold for artikkel 25 i nevnte forordning.

Artikkel 24

Vilkår for registrering av meldinger om nektet innreise og opphold

1. Medlemsstatene skal registrere en melding om nektet innreise og opphold når et av følgende vilkår er oppfylt:

(a) Medlemsstaten har på grunnlag av en individuell vurdering som omfatter en vurdering av den berørte tredjestatsborgerens personlige omstendigheter og konsekvenser av å nekte vedkommende innreise og opphold, fastslått at tredjestatsborgerens tilstedeværelse på dens territorium utgjør en trussel mot den offentlige orden, den offentlige sikkerhet eller den nasjonale sikkerhet, og medlemsstaten har derfor vedtatt en rettslig eller administrativ beslutning i samsvar med sin nasjonale rett om å nekte innreise og opphold og utstedt en nasjonal melding om nektet innreise og opphold.

(b) Medlemsstaten har utstedt et innreiseforbud for en tredjestatsborger i samsvar med framgangsmåter som overholder direktiv 2008/115/EF.

2. Situasjonene omfattet av nr. 1 bokstav a) skal oppstå når

(a) en tredjestatsborger i en medlemsstat er blitt idømt en frihetsstraff med varighet på minst ett år på grunn av et straffbart forhold,

(b) det er alvorlig grunn til mistanke om at en tredjestatsborger har begått et alvorlig straffbart forhold, herunder en terrorhandling, eller når det foreligger klare holdepunkter for at vedkommende har til hensikt å begå et straffbart forhold på en medlemsstats territorium, eller

(c) en tredjestatsborger har omgått eller forsøkt å omgå unionsretten eller nasjonal rett om innreise og opphold på medlemsstatenes territorium.

3. Den innmeldende medlemsstat skal sikre at meldingen er synlig i SIS så snart den berørte tredjestatsborgeren har forlatt medlemsstatenes territorium, eller så snart som mulig dersom den innmeldende medlemsstat har fått klare holdepunkter for at tredjestatsborgeren har forlatt medlemsstatenes territorium, med sikte på å hindre at denne tredjestartsstatsborgeren reiser inn igjen.

4. Personer som er gjenstand for en beslutning om nektet innreise og opphold som nevnt i nr. 1, skal ha klageadgang. Slike klagesaker skal behandles i samsvar med unionsretten og nasjonal rett og skal omfatte en effektiv klageadgang ved en domstol.

Artikkel 25

Vilkår for registrering av meldinger om tredjestatsborgere som er omfattet av restriktive tiltak

1. Meldinger om tredjestatsborgere som omfattes av restriktive tiltak for å hindre innreise til eller transitt gjennom medlemsstatenes territorium, truffet i henhold til rettsakter vedtatt av Rådet, herunder tiltak for å gjennomføre reiseforbud utstedt av De forente nasjoners sikkerhetsråd, skal registreres i SIS for å nekte innreise eller opphold, forutsatt at kravene til opplysningenes kvalitet er oppfylt.

2. Meldingene skal registreres, ajourføres og slettes av vedkommende myndighet i medlemsstaten som har formannskapet for Rådet for Den europeiske union på tidspunktet tiltaket vedtas. Dersom denne medlemsstaten ikke har tilgang til SIS eller til meldinger registrert i samsvar med denne forordning, skal ansvaret påhvile medlemsstaten som har formannskapet i den påfølgende perioden, og som har tilgang til SIS, herunder meldinger registrert i samsvar med denne forordning.

Medlemsstatene skal innføre nødvendige framgangsmåter for å registrere, ajourføre og slette slike meldinger.

Artikkel 26

Vilkår for registrering av meldinger om tredjestatsborgere som omfattes av retten til fri bevegelighet innenfor Unionen

1. En melding om en tredjestatsborger som omfattes av retten til fri bevegelighet innenfor Unionen i henhold til direktiv 2004/38/EF eller en avtale mellom Unionen eller Unionen og dens medlemsstater på den ene side og en tredjestat på den annen side, skal være i samsvar med reglene vedtatt for gjennomføring av nevnte direktiv eller avtale.

2. Ved treff på en melding registrert i henhold til artikkel 24 om en tredjestatsborger som omfattes av retten til fri bevegelighet innenfor Unionen, skal den fullbyrdende medlemsstaten umiddelbart rådføre seg med den innmeldende medlemsstaten via utveksling av utfyllende opplysninger for omgående å avgjøre hvilke tiltak som skal treffes.

Artikkel 27

Samråd før utstedelse eller forlengelse av en oppholdstillatelse eller et visum for langvarig opphold

Dersom en medlemsstat vurderer å utstede eller forlenge en oppholdstillatelse eller et visum for langvarig opphold til en tredjestatsborger som er gjenstand for en melding om nektet innreise og opphold som er registrert av en annen medlemsstat, skal de berørte medlemsstatene rådføre seg med hverandre ved utveksling av utfyllende opplysninger i samsvar med følgende regler:

(a) Den utstedende medlemsstaten skal rådføre seg med den innmeldende medlemsstaten før den utsteder eller forlenger oppholdstillatelsen eller visumet for langvarig opphold.

(b) Den innmeldende medlemsstaten skal svare på anmodningen om samråd innen ti kalenderdager.

(c) Dersom det ikke gis svar innen fristen i bokstav b), skal det innebære at den innmeldende medlemsstaten ikke motsetter seg utstedelsen eller forlengelsen av oppholdstillatelsen eller visumet for langvarig opphold.

(d) Når den utstedende medlemsstat treffer den relevante beslutningen, skal den ta hensyn til begrunnelsene for den innmeldende medlemsstatens beslutning og vurdere i samsvar med nasjonal rett enhver trussel mot den offentlige orden eller den offentlige sikkerhet som den berørte tredjestatsborgerens tilstedeværelse på medlemsstatenes territorium kan utgjøre.

(e) Den utstedende medlemsstaten skal underrette den innmeldende medlemsstaten om sin beslutning.

(f) Dersom den utstedende medlemsstaten underretter den innmeldende medlemsstaten om at den har til hensikt å utstede eller forlenge oppholdstillatelsen eller visumet for langvarig opphold, eller at den har besluttet å gjøre det, skal den innmeldende medlemsstaten slette meldingen om nektet innreise og opphold.

Den endelige beslutningen om hvorvidt det skal utstedes en oppholdstillatelse eller et visum for langvarig opphold til en tredjestatsborger, påhviler den utstedende medlemsstaten.

Artikkel 28

Samråd før registrering av en melding om nektet innreise og opphold

Dersom en medlemsstat har truffet en beslutning i henhold til artikkel 24 nr. 1 og vurderer å registrere en melding om nektet innreise og opphold for en tredjestatsborger som innehar en gyldig oppholdstillatelse eller et gyldig visum for langvarig opphold utstedt av en annen medlemsstat, skal de berørte medlemsstatene rådføre seg med hverandre ved utveksling av utfyllende opplysninger i samsvar med følgende regler:

(a) Medlemsstaten som har truffet beslutningen nevnt i artikkel 24 nr. 1, skal underrette den utstedende medlemsstaten om beslutningen.

(b) Opplysningene utvekslet i henhold til bokstav a) i denne artikkel skal inneholde tilstrekkelig informasjon om begrunnelsene for beslutningen nevnt i artikkel 24 nr. 1.

(c) På grunnlag av opplysningene fra medlemsstaten som har truffet beslutningen nevnt i artikkel 24 nr. 1, skal den utstedende

medlemsstaten vurdere om det er grunnlag for å tilbakekalle oppholdstillatelsen eller visumet for langvarig opphold.

(d) Når den utstedende medlemsstaten treffer den relevante beslutningen, skal den ta hensyn til begrunnelsene for beslutningen til medlemsstaten som har truffet beslutningen nevnt i artikkel 24 nr. 1, og vurdere i samsvar med nasjonal rett enhver trussel mot den offentlige orden eller den offentlige sikkerhet som den berørte tredjestatsborgerens tilstedeværelse på medlemsstatenes territorium kan utgjøre.

(e) Den utstedende medlemsstaten skal innen 14 kalenderdager etter å ha mottatt anmodning om samråd underrette medlemsstaten som har truffet beslutningen nevnt i artikkel 24 nr. 1, om sin beslutning eller inngi, dersom det har vært umulig for den utstedende medlemsstaten å treffe en beslutning innen denne fristen, en begrunnet anmodning om unntaksvis å forlenge fristen for sitt svar med ytterligere høyst 12 kalenderdager.

(f) Dersom den utstedende medlemsstaten underretter medlemsstaten som har truffet beslutningen nevnt i artikkel 24 nr. 1 om at den opprettholder oppholdstillatelsen eller visumet for langvarig opphold, skal ikke medlemsstaten som har truffet beslutningen, registrere meldingen om nektet innreise og opphold.

Artikkel 29

Samråd etter registrering av en melding om nektet innreise og opphold

Dersom det viser seg at en medlemsstat har registrert et treff på en melding om nektet innreise og opphold for en tredjestatsborger som innehar en gyldig oppholdstillatelse eller et gyldig visum for langvarig opphold utstedt av en annen medlemsstat, skal de berørte medlemsstatene rådføre seg med hverandre ved utveksling av utfyllende opplysninger i samsvar med følgende regler:

(a) Den innmeldende medlemsstaten skal underrette den utstedende medlemsstaten om meldingen om nektet innreise og opphold.

(b) Opplysningene utvekslet i henhold til bokstav a) skal inneholde tilstrekkelig informasjon om begrunnelsene for meldingen om nektet innreise og opphold.

(c) På grunnlag av opplysningene fra den innmeldende medlemsstaten, skal den utstedende medlemsstaten vurdere om det er grunnlag for å tilbakekalle oppholdstillatelsen eller visumet for langvarig opphold.

(d) Når den utstedende medlemsstat treffer sin beslutning, skal den ta den hensyn til begrunnelsene for den innmeldende medlemsstats beslutning og vurdere i samsvar med nasjonal rett enhver trussel mot den offentlige orden eller den offentlige sikkerhet som den berørte tredjestatsborgerens tilstedeværelse på medlemsstatenes territorium kan utgjøre.

(e) Den utstedende medlemsstaten skal innen 14 kalenderdager etter å ha mottatt anmodning om samråd underrette den innmeldende medlemsstaten om sin beslutning eller inngi, dersom det har vært umulig for den utstedende medlemsstaten å treffe en beslutning innen denne fristen, en begrunnet anmodning om unntaksvis å forlenge fristen for sitt svar med ytterligere høyst 12 kalenderdager.

(f) Dersom den utstedende medlemsstaten underretter den innmeldende medlemsstaten om at den opprettholder oppholdstillatelsen eller visumet for langvarig opphold, skal den innmeldende medlemsstaten umiddelbart slette meldingen om nektet innreise og opphold.

Artikkel 30

Samråd ved et treff om en tredjestatsborger som innehar en gyldig oppholdstillatelse eller et gyldig visum for langvarig opphold

Dersom en medlemsstat får et treff på en melding om nektet innreise og opphold registrering av en medlemsstat for en tredjestatsborger som innehar en gyldig oppholdstillatelse eller et gyldig visum for langvarig opphold utstedt av en annen medlemsstat, skal de berørte medlemsstatene rådføre seg med hverandre ved utveksling av utfyllende opplysninger i samsvar med følgende regler:

(a) Den fullbyrdende medlemsstaten skal underrette den innmeldende medlemsstaten om situasjonen.

(b) Den innmeldende medlemsstaten skal innlede framgangsmåten fastsatt i artikkel 29.

(c) Den innmeldende medlemsstaten skal underrette den fyllbyrdende medlemsstaten om det endelige resultatet av samrådet.

Beslutningen om den berørte tredjestatsborgerens innreise skal treffes av den fullbyrdende medlemsstaten i samsvar med forordning (EU) 2016/399.

Artikkel 31

Statistikk over utveksling av opplysninger

Medlemsstatene skal hvert år framlegge statistikk for eu-LISA over de utvekslinger av opplysninger som er gjennomført i samsvar med artikkel 27–30, og over tilfeller der fristene i de nevnte artiklene ikke ble overholdt.

KAPITTEL VI

SØK MED BIOMETRISKE OPPLYSNINGER

Artikkel 32

Særlige regler for registrering av fotografier, ansiktsbilder og fingeravtrykksopplysninger

1. Bare fotografier, ansiktsbilder og fingeravtrykksopplysninger i henhold til artikkel 20 nr. 2 bokstav w) og x) som oppfyller minstestandarder for opplysningers kvalitet og tekniske spesifikasjoner, skal registreres i SIS. Før disse opplysningene registreres, skal det utføres en kvalitetskontroll for å fastslå om minstestandardene for opplysningers kvalitet og tekniske spesifikasjoner er oppfylt.

2. Fingeravtrykksopplysninger som registreres i SIS, kan bestå av ett–ti flate fingeravtrykk og ett–ti rullede fingeravtrykk. De kan også omfatte inntil to håndflateavtrykk.

3. Minstestandarder for opplysningers kvalitet og tekniske spesifikasjoner for lagring av de biometriske opplysningene nevnt i nr. 1 i denne artikkel skal fastsettes i samsvar med nr. 4 i denne artikkel. Disse minstestandarder for opplysningers kvalitet og tekniske spesifikasjoner skal fastsette det kvalitetsnivå som kreves for å bruke opplysningene til å kontrollere en person identitet i samsvar med artikkel 33 nr. 1 og for å bruke opplysningene til å identifisere en person i samsvar med artikkel 33 nr. 2–4.

4. Kommisjonen skal vedta gjennomføringsrettsakter for å fastsette minstestandardene for opplysningers kvalitet og tekniske spesifikasjoner nevnt i nr. 1 og 3 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

Artikkel 33

Særlige regler for kontroll eller søk med fotografier, ansiktsbilder og fingeravtrykksopplysninger

1. Når en melding i SIS inneholder fotografier, ansiktsbilder og fingeravtrykksopplysninger, skal slike fotografier, ansiktsbilder og fingeravtrykksopplysninger brukes til å bekrefte identiteten til en person som er funnet som følge av et alfanumerisk søk i SIS.

2. Det kan i alle tilfeller søkes på fingeravtrykksopplysninger for å identifisere en person. Det skal imidlertid søkes på fingeravtrykksopplysninger for å identifisere en person dersom personens identitet ikke kan fastslås på annen måte. For det formål skal det sentrale SIS inneholde et system for automatisert fingeravtrykksidentifisering (AFIS).

3. Det kan også søkes i fingeravtrykksopplysninger i SIS i forbindelse med meldinger som er registrert i samsvar med artikkel 24 og 25, ved bruk av fullstendige eller ufullstendige sett av fingeravtrykk eller håndflateavtrykk som er funnet på et åsted under etterforskning av grov kriminalitet eller terrorhandlinger, dersom det med stor sannsynlighet kan fastslås at disse settene av avtrykk tilhører en gjerningsperson, og forutsatt at søket foretas samtidig i medlemsstatens relevante nasjonale fingeravtrykksdatabaser.

4. Fotografier og ansiktsbilder kan brukes til å identifisere en person ved alminnelige grenseoverganger så snart det blir teknisk mulig, og forutsatt at det sikres at identifiseringen er svært pålitelig.

Før denne funksjonen gjennomføres i SIS, skal Kommisjonen framlegge en rapport om den nødvendige teknologien er tilgjengelig, klar til bruk og pålitelig. Europaparlamentet skal rådspørres om rapporten.

Etter at funksjonen er tatt i bruk ved alminnelige grenseoverganger, skal Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 61 for å utfylle denne forordning om fastsettelse av hvilke andre omstendigheter fotografier og ansiktsbilder kan brukes under til å identifisere personer.

KAPITTEL VII

TILGANGSRETT OG UNDERSØKELSE OG SLETTING AV MELDINGER

Artikkel 34

Nasjonale vedkommende myndigheter med tilgangsrett til opplysninger i SIS

1. Nasjonale vedkommende myndigheter med ansvar for å identifisere tredjestatsborgere skal ha tilgang til opplysninger som er registrert i SIS, og rett til å søke direkte i disse opplysningene eller i en kopi av SIS-databasen for følgende formål:

a) grensekontroll i samsvar med forordning (EU) 2016/399,

b) politi- og tollkontroller innenfor den berørte medlemsstaten og utpekte myndigheters samordning av slike kontroller,

(c) forebygging, avsløring, etterforskning eller rettsforfølging av terrorhandlinger eller andre alvorlige straffbare forhold eller fullbyrding av strafferettslige sanksjoner i den berørte medlemsstaten, forutsatt at direktiv (EU) 2016/680 får anvendelse,

(d) undersøkelse av vilkårene og beslutningstaking i forbindelse med tredjestatsborgeres innreise og opphold på medlemsstatenes territorium, herunder når det gjelder oppholdstillatelser og visum for langvarig opphold og tilbakesending av tredjestatsborgere samt utføring av kontroller av tredjestatsborgere som reiser inn eller oppholder seg ulovlig på medlemsstatenes territorium,

(e) sikkerhetskontroller av tredjestatsborgere som søker om internasjonal beskyttelse dersom myndighetene som utfører kontrollene, ikke er «besluttende myndigheter» som definert i artikkel 2 bokstav f) i europaparlaments- og rådsdirektiv 2013/32/EU ([1]) og eventuelt rådgivning i samsvar med rådsforordning (EF) nr. 377/2004 ([2]),

(f) behandling av visumsøknader og beslutninger om disse, herunder om visum skal annulleres, inndras eller forlenges i samsvar med europaparlaments- og rådsforordning (EF) nr. 810/2009 ([3]).

2. Tilgangsretten til opplysninger i SIS og retten til å søke direkte i slike opplysninger kan ved behandling av en søknad om naturalisering utøves av nasjonale vedkommende myndigheter med ansvar for naturalisering i henhold til nasjonal rett.

3. Ved anvendelse av artikkel 24 og 25 kan tilgangsretten til opplysninger i SIS og retten til å søke direkte i slike opplysninger også utøves av nasjonale rettsmyndigheter, herunder påtalemyndigheten og politimyndigheten, når de utfører sine oppgaver i henhold til nasjonal rett samt deres samordningsmyndigheter.

4. Tilgangsrett til opplysninger om dokumenter om personer som er registrert i samsvar med artikkel 38 nr. 2 bokstav k) og l) i forordning (EU) 2018/1862, og rett til å søke i disse opplysningene, kan også utøves av myndighetene nevnt i nr. 1 bokstav f) i denne artikkel.

5. Vedkommende myndigheter omhandlet i denne artikkel skal tas med i listen i artikkel 41 nr. 8.

Artikkel 35

Europols tilgang til opplysninger i SIS

1. Den europeiske unions byrå for politisamarbeid (Europol), opprettet ved forordning (EU) 2016/794, skal, dersom det er nødvendig for at Europol skal oppfylle sitt mandat, ha tilgangsrett til og rett til å søke i opplysninger i SIS. Europol kan også utveksle og anmode om utfyllende opplysninger i samsvar med bestemmelsene i SIRENE-håndboken.

2. Dersom et søk foretatt av Europol viser at det finnes en melding i SIS, skal Europol underrette den innmeldende medlemsstaten via utveksling av utfyllende opplysninger ved hjelp av kommunikasjonsinfrastrukturen og i samsvar med bestemmelsene i SIRENE-håndboken. Inntil Europol kan bruke funksjonene for utveksling av utfyllende opplysninger, skal Europol underrette den innmeldende medlemsstaten via kanalene fastsatt i forordning (EU) 2016/794.

3. Europol kan behandle de utfyllende opplysningene som er oversendt fra medlemsstater for å sammenligne dem med sine databaser og prosjekter for operative analyser som skal finne sammenhenger eller andre relevante koplinger, og for analyser av strategisk, tematisk eller operativ art som nevnt i artikkel 18 nr. 2 bokstav a), b) og c) i forordning (EU) 2016/794. Enhver behandling av utfyllende opplysninger foretatt av Europol i henhold til denne artikkel skal utføres i samsvar med nevnte forordning.

4. Europols bruk av opplysninger fra søk i SIS eller fra behandling av utfyllende opplysninger skal kreve den innmeldende medlemsstatens samtykke. Dersom medlemsstaten tillater at slike opplysninger brukes, skal Europols behandling av dem skje i samsvar med forordning (EU) 2016/794. Europol skal underrette tredjestater og tredjeorganer om slike opplysninger bare med den innmeldende medlemsstatens samtykke og i fullt samsvar med unionsretten om personvern.

(1) Europaparlaments- og rådsdirektiv 2013/32/EU av 26. juni 2013 om felles framgangsmåter for tildeling og tilbakekalling av internasjonal beskyttelse (EUT L 180 av 29.6.2013, s. 60).
(2) Rådsforordning (EF) nr. 377/2004 av 19. februar 2004 om opprettelse av et nettverk av kontaktpersoner for innvandringssaker (EUT L 64 av 2.3.2004, s. 1).
(3) Europaparlaments- og rådsforordning (EF) nr. 810/2009 av 13. juli 2009 om innføring av fellesskapsregler for visum (visumregler) (EUT L 243 av 15.9.2009, s. 1).

5. Europol skal

(a) uten at det berører nr. 4 og 6, ikke kople deler av SIS til, eller overføre de opplysninger i SIS som Europol har tilgang til, til noe system for innsamling og behandling av opplysninger drevet av eller ved Europol, eller laste ned eller på annen måte kopiere deler av SIS,

(b) uten hensyn til artikkel 31 nr. 1 i forordning (EU) 2016/794 slette utfyllende opplysninger som inneholder personopplysninger senest ett år etter at den tilhørende meldingen er slettet. Som et unntak kan Europol, dersom Europol har opplysninger i sine databaser eller prosjekter for operative analyser om en sak med tilknytning til de utfyllende opplysningene, for å kunne utføre sine oppgaver unntaksvis fortsatt lagre de utfyllende opplysningene dersom det er nødvendig. Europol skal underrette den innmeldende og fullbyrdende medlemsstaten om den fortsatte lagring av slike utfyllende opplysninger og begrunne dette,

(c) begrense tilgangen til opplysninger i SIS, herunder utfyllende opplysninger, til Europol-personale med særskilt fullmakt som har bruk for tilgang til slike opplysninger for å kunne utføre sine oppgaver,

(d) vedta og anvende tiltak for å ivareta sikkerheten, fortroligheten og egenkontrollen i samsvar med artikkel 10, 11 tilog 13,

(e) sikre at personale med fullmakt til å behandle SIS-opplysninger får relevant opplæring og informasjon i samsvar med artikkel 14 nr. 1, og

(f) uten at det berører forordning (EU) 2016/794, la EUs datatilsyn overvåke og undersøke Europols aktiviteter når det utøver sin tilgangsrett og rett til å søke i opplysninger i SIS og utveksle og behandle utfyllende opplysninger.

6. Europol skal kopiere opplysninger fra SIS bare for tekniske formål, dersom dette er nødvendig for at Europol-personale med tilstrekkelig fullmakt kan foreta et direkte søk. Denne forordning skal også gjelde slike kopier. Den tekniske kopien skal brukes bare for å lagre SIS-opplysninger mens det søkes i disse opplysningene. Når det er søkt i opplysningene, skal de slettes. Slik bruk skal ikke anses som ulovlig nedlasting eller kopiering av SIS-opplysninger. Europol skal ikke kopiere meldingsopplysninger eller tilleggsopplysninger fra medlemsstater eller CS-SIS til andre Europol-systemer.

7. Europol skal i samsvar med bestemmelsene i artikkel 12 føre logger over hver tilgang til og hvert søk i SIS for å kontrollere om behandlingen av opplysninger skjer på lovlig vis, utøve egenkontroll og ivareta opplysningers sikkerhet og integritet. Disse loggene og denne dokumentasjonen skal ikke anses som ulovlig nedlasting eller kopiering fra en del av SIS.

8. Medlemsstatene skal underrette Europol via utveksling av utfyllende opplysninger om eventuelle treff på meldinger i forbindelse med terrorhandlinger. Medlemsstatene kan unntaksvis unnlate å underrette Europol dersom dette ville sette igangværende etterforskninger eller en fysisk persons sikkerhet i fare eller være i strid med vesentlige sikkerhetsinteresser i den innmeldende medlemsstaten.

9. Nr. 8 får anvendelse fra den dato Europol kan motta utfyllende opplysninger i samsvar med nr. 1.

Artikkel 36

Tilgang til opplysninger i SIS for europeiske grense- og kystvaktenheter, enheter med personale som arbeider med tilbakesending, og medlemmene av støttegruppene for migrasjonsstyring

1. I samsvar med artikkel 40 nr. 8 i forordning (EU) 2016/1624 skal medlemmene i enhetene nevnt i artikkel 2 nr. 8 og 9 i nevnte forordning i sitt mandat, og forutsatt at de har tillatelse til å foreta kontroller i henhold til artikkel 34 nr. 1 i denne forordning og har fått nødvendig opplæring i henhold til artikkel 14 nr. 1 i denne forordning, ha tilgangsrett og rett til søk i opplysninger i SIS dersom det er nødvendig for at de skal kunne utføre sin oppgave, og i den grad det kreves i henhold til driftsplanen for en spesifikk operasjon. Tilgang til opplysninger i SIS skal ikke utvides til andre medlemmer i enheten.

2. Medlemmene i enhetene nevnt i nr. 1 skal utøve tilgangsretten og retten til å søke i opplysninger i SIS i samsvar med nr. 1 via et teknisk grensesnitt. Det tekniske grensesnittet skal opprettes og vedlikeholdes av Det europeiske grense- og kystvaktbyrå og skal sikre en direkte forbindelse til det sentrale SIS.

3. Når et søk foretatt av et medlem i enhetene nevnt i nr. 1 i denne artikkel viser at det foreligger en melding i SIS, skal den innmeldende medlemsstaten underrettes om dette. I samsvar med artikkel 40 i forordning (EU) 2016/1624 skal medlemmer i enhetene bare reagere på en melding i SIS i henhold til instruksene fra og som hovedregel i nærvær av grensevakter eller personale som arbeider med tilbakesending i vertsmedlemsstaten der de opererer. Vertsmedlemsstaten kan gi medlemmene av enhetene tillatelse til å handle på dens vegne.

4. Det europeiske grense- og kystvaktbyrå skal i samsvar med bestemmelsene i artikkel 12 føre logger over hver tilgang til og hvert søk i SIS for å kontrollere om behandlingen av opplysninger skjer på lovlig vis, utøve egenkontroll og ivareta opplysningers sikkerhet og integritet.

5. Det europeiske grense- og kystvaktbyrå skal vedta og anvende tiltak for å ivareta sikkerheten, fortroligheten og egenkontrollen i samsvar med artikkel 10, 11 og 13 og skal sikre at enhetene nevnt i nr. 1 i denne artikkel anvender disse tiltakene.

6. Ingenting i denne artikkel skal forstås slik at det berører bestemmelsene i forordning (EU) 2016/1624 om vern av personopplysninger eller Det europeiske grense- og kystvaktbyrås ansvar for sin uautoriserte eller uriktige behandling av opplysninger.

7. Uten at det berører nr. 2, skal ingen deler av SIS koples til noe system for innsamling eller behandling av opplysninger som drives av enhetene nevnt i nr. 1 eller av Det europeiske grense- og kystvaktbyrå, og heller ikke skal opplysningene i SIS som enhetene har tilgang til, overføres til et slikt system. Ingen del av SIS skal lastes ned eller kopieres. Loggføringen av tilgang og søk skal ikke anses som ulovlig nedlasting eller kopiering av SIS-opplysninger.

8. Det europeiske grense- og kystvaktbyrå skal tillate at EUs datatilsyn overvåker og undersøker virksomheten til enhetene

nevnt i denne artikkel når de utøver sin tilgangsrett og rett til å søke i opplysninger i SIS. Dette skal ikke berøre de ytterligere bestemmelsene i forordning (EU) 2018/1725.

Artikkel 37

Evaluering av Europols og Det europeiske grense- og kystvaktbyrås bruk av SIS

1. Kommisjonen skal utføre en evaluering minst hvert femte år av driften og bruken av SIS av Europol og enhetene nevnt i artikkel 36 nr. 1.

2. Europol og Det europeiske grense- og kystvaktbyrå skal sikre en passende oppfølging av resultatene og anbefalingene fra evalueringen.

3. En rapport om resultatene av evalueringen og oppfølgingen av den skal oversendes til Europaparlamentet og Rådet.

Artikkel 38

Tilgangens omfang

Sluttbrukerne, herunder Europol og medlemmene i enhetene nevnt i artikkel 2 nr. 8 og 9 i forordning (EU) 2016/1624, skal ha tilgang bare til opplysninger de trenger for å utføre sine oppgaver.

Artikkel 39

Undersøkelsesfrist for meldinger

1. Meldinger skal lagres bare så lenge det er nødvendig for å oppnå formålene som ligger til grunn for registreringen.

2. En innmeldende medlemsstat skal innen tre år etter at en melding er registrert i SIS, undersøke om det er behov for fortsatt lagring. Dersom det i den nasjonale beslutning som ligger til grunn for meldingen, fastsettes en lengre gyldighetsperiode enn tre år, skal meldingen undersøkes innen fem år.

3. Hver medlemsstat skal, dersom det er relevant, fastsette kortere undersøkelsesfrister i samsvar med nasjonal rett.

4. Den innmeldende medlemsstaten kan innen undersøkelsesfristen etter en omfattende individuell vurdering, som skal dokumenteres, beslutte å lagre meldingen lenger enn undersøkelsesfristen dersom dette er nødvendig og står i forhold til formålene som ligger til grunn for meldingen. I så fall kommer nr. 2 til anvendelse også for den utvidede perioden. En slik forlengelse skal meddeles CS-SIS.

5. Meldinger skal automatisk slettes etter at undersøkelsesfristen i nr. 2 er utløpt, med mindre den innmeldende medlemsstaten har underrettet CS-SIS om en forlengelse i henhold til nr. 4. CS-SIS skal automatisk underrette medlemsstatene om enhver planlagt sletting av opplysninger med fire måneders varsel.

6. Medlemsstatene skal føre statistikk over antall meldinger hvis lagringstid er forlenget i samsvar med nr. 4 i denne artikkel, og på anmodning oversende dem til tilsynsmyndighetene nevnt i artikkel 55.

7. Så snart det står klart for et SIRENE-kontor at en melding har oppfylt sitt formål og derfor bør slettes, skal det umiddelbart underrette myndigheten som opprettet meldingen. Myndigheten skal ha 15 kalenderdager fra denne underretningen er mottatt til å svare at meldingen er blitt eller vil bli slettet, eller begrunne hvorfor meldingen fortsatt lagres. Dersom det ikke mottas et svar innen 15-dagersfristen, skal SIRENE-kontoret sikre at meldingen slettes. Dersom det er tillatt i henhold til nasjonal rett, skal SIRENE-kontoret slette meldingen. SIRENE-kontorene skal melde eventuelle gjentatte problemer som de støter på når de utøver dette nummer, til sin tilsynsmyndighet.

Artikkel 40

Sletting av meldinger

1. Meldinger om nektet innreise og opphold i henhold til artikkel 24 skal slettes

(a) når beslutningen som lå til grunn for å registrere meldingen, er blitt tilbakekalt eller annullert av vedkommende myndighet, eller

(b) dersom det er relevant, på bakgrunn av samrådsordningen nevnt i artikkel 27 og artikkel 29.

2. Meldinger om tredjestatsborgere som omfattes av restriktive tiltak for å hindre innreise til eller transitt gjennom medlemsstatenes territorium, skal slettes når de restriktive tiltakene er avsluttet, suspendert eller annullert.

3. Meldinger om en person som har oppnådd statsborgerskap i en medlemsstat eller enhver stat hvis statsborgere omfattes av retten til fri bevegelighet i henhold til unionsretten, skal slettes så snart den innmeldende medlemsstaten blir klar over eller underrettes i henhold til artikkel 44 om at vedkommende har oppnådd et slikt statsborgerskap.

4. Meldingen skal slettes når meldingen utløper i samsvar med artikkel 39.

KAPITTEL VIII

GENERELLE REGLER FOR BEHANDLING AV OPPLYSNINGER

Artikkel 41

Behandling av opplysninger i SIS

1. Medlemsstatene skal behandle opplysningene omhandlet i artikkel 20 bare for å nekte innreise til og opphold på deres territorium.

2. Kopier av opplysningene skal lages bare for tekniske formål, og bare dersom dette er nødvendig for at vedkommende myndigheter omhandlet i artikkel 34 skal kunne foreta direkte søk. Denne forordning skal gjelde disse kopiene. En medlemsstat skal ikke kopiere meldingsopplysninger eller tilleggsopplysninger som en annen medlemsstat har registrert fra sitt N.SIS eller fra CS-SIS til andre nasjonale datafiler.

3. Tekniske kopier i henhold til nr. 2 som fører til frakoplede databaser, kan ikke lagres i mer enn 48 timer.

Uten hensyn til første ledd skal tekniske kopier som fører til frakoplede databaser, og som skal brukes av visumutstedende myndigheter, ikke lenger være tillatt, med forbehold for kopier som lages for bruk i en nødsituasjon dersom nettverket har vært utilgjengelig i mer enn 24 timer.

Medlemsstatene skal lagre en oppdatert oversikt over slike kopier, gjøre denne oversikten tilgjengelig for sine tilsynsmyndigheter og påse at denne forordning, særlig artikkel 10, kommer til anvendelse på slike kopier.

4. Tilgang til opplysninger i SIS for nasjonale vedkommende myndigheter nevnt i artikkel 34 skal bare tillates innenfor rammen av deres fullmakter og bare til behørig autorisert personale.

5. All behandling av opplysningene i SIS for andre formål enn de som lå til grunn for registreringen i SIS, skal være koplet til en bestemt sak og være begrunnet med at det er nødvendig å forebygge en overhengende og alvorlig fare for den offentlige orden og sikkerhet, en alvorlig trussel mot statens sikkerhet eller et alvorlig straffbart forhold. I et slikt tilfelle skal det innhentes tillatelse fra den innmeldende medlemsstaten på forhånd.

6. Opplysninger om dokumenter om personer som er registrert i SIS i henhold til artikkel 38 nr. 2 bokstav k) og l) i forordning (EU) 2018/1862, kan brukes av vedkommende myndigheter nevnt i artikkel 34 nr. 1 bokstav f) i samsvar med lovene i hver medlemsstat.

7. Enhver bruk av SIS-opplysninger som ikke er i samsvar med nr. 1–6, skal anses som misbruk i henhold til den enkelte medlemsstats nasjonale rett og underlagt strafferettslige sanksjoner i henhold til artikkel 59.

8. Hver medlemsstat skal oversende til eu-LISA en liste over vedkommende myndigheter som har tillatelse til å søke direkte i opplysningene i SIS i henhold til denne forordning samt enhver endring i denne listen. Listen skal for hver myndighet spesifisere hvilke opplysninger den kan søke i og for hvilke formål. eu-LISA skal sørge for at listen offentliggjøres i Den europeiske unions tidende hvert år. eu-LISA skal på sitt nettsted føre en liste som løpende ajourføres, med de endringer som medlemsstatene har oversendt mellom de årlige offentliggjøringer.

9. Dersom det ikke fastsettes særlige bestemmelser i unionsretten, skal den enkelte medlemsstats rett komme til anvendelse på opplysninger i N.SIS.

Artikkel 42

Opplysninger i SIS og nasjonale filer

1. Artikkel 41 nr. 2 skal ikke berøre en medlemsstats rett til å lagre i sine nasjonale filer SIS-opplysninger om tiltak som har blitt truffet på dens territorium. Slike opplysninger skal lagres i nasjonale filer i høyst tre år, med mindre nasjonal rett inneholder særlige bestemmelser om lengre lagringstid.

2. Artikkel 41 nr. 2 skal ikke berøre en medlemsstats rett til å lagre i sine nasjonale filer opplysninger i en bestemt melding som medlemsstaten har registrert i SIS.

Artikkel 43

Opplysninger dersom en melding ikke blir gjennomført

Dersom et tiltak det anmodes om, ikke kan gjennomføres, skal medlemsstaten som anmodes om å treffe tiltaket, straks underrette den innmeldende medlemsstaten via utveksling av utfyllende opplysninger.

Artikkel 44

Kvaliteten på opplysningene i SIS

1. Den innmeldende medlemsstaten skal være ansvarlig for at opplysningene er adekvate, ajourført og lovlig registrert i SIS.

2. Dersom en innmeldende medlemsstat mottar relevante utfyllende eller endrede opplysninger som angitt i artikkel 20 nr. 2, skal den uten opphold fullføre eller endre meldingen.

3. Bare den innmeldende medlemsstaten har myndighet til å endre, utfylle, rette, ajourføre eller slette opplysninger den har registrert i SIS.

4. Dersom en annen medlemsstat enn den innmeldende medlemsstat har relevante utfyllende eller endrede opplysninger som angitt i artikkel 20 nr. 2, skal den uten opphold oversende dem via utveksling av utfyllende opplysninger til den innmeldende medlemsstat, slik at den kan fullføre eller endre meldingen. Opplysningene skal bare overføres dersom tredjestatsborgerens identitet kan fastslås.

5. Dersom en annen medlemsstat enn den innmeldende medlemsstat har holdepunkter for at en opplysning inneholder faktiske feil eller er urettmessig registrert, skal den via utveksling av utfyllende opplysninger underrette den innmeldende medlemsstaten snarest mulig og senest to virkedager etter at den fikk kjennskap til dette. Den innmeldende medlemsstaten skal undersøke opplysningene og om nødvendig omgående rette eller slette opplysningen.

6. Dersom medlemsstatene ikke kommer til enighet innen to måneder etter at dokumentasjonen ble kjent som nevnt i nr. 5 i denne artikkel, skal medlemsstaten som ikke har registrert meldingen, framlegge saken for de berørte tilsynsmyndighetene og EUs datatilsyn for å få truffet en beslutning ved hjelp av samarbeid i samsvar med artikkel 57.

7. Medlemsstatene skal utveksle utfyllende opplysninger dersom en person påklager at vedkommede ikke er den tiltenkte gjenstand for en melding. Dersom resultatet av kontrollen viser at den tiltenkte gjenstand for en melding ikke er klageren, skal klageren underrettes om tiltakene fastsatt i artikkel 47 og om klageadgangen i henhold til artikkel 54 nr. 1.

Artikkel 45

Sikkerhetshendelser

1. Enhver hendelse som har eller kan ha innvirkning på sikkerheten i SIS eller kan forårsake skade på eller tap av SIS-opplysninger eller utfyllende opplysninger, skal anses for å være en sikkerhetshendelse, særlig når det kan ha vært ulovlig adgang til opplysninger, eller dersom opplysningenes tilgjengelighet, integritet og fortrolighet er eller kan ha blitt satt i fare.

2. Sikkerhetshendelser skal håndteres slik at en rask, effektiv og passende reaksjon sikres.

3. Uten at det berører underrettelsen og meddelelsen av et brudd på personopplysningssikkerheten i henhold til artikkel 33 i forordning (EU) 2016/679 eller artikkel 30 i direktiv (EU) 2016/680, skal medlemsstatene, Europol og Det europeiske grense- og kystvaktbyrå omgående underrette Kommisjonen, eu-LISA, vedkommende tilsynsmyndighet og EUs datatilsyn om eventuelle sikkerhetshendelser i forbindelse med det sentrale SIS.

4. Opplysninger om en sikkerhetshendelse som har eller kan ha innvirkning på driften av SIS i en medlemsstat eller innenfor eu-LISA, på tilgjengeligheten, integriteten og fortroligheten av opplysninger som registreres eller sendes av andre medlemsstater, eller de utfyllende opplysningene som utveksles, skal straks framlegges for alle medlemsstatene og meldes i samsvar med hendelsesstyringsplanen som skal utarbeides av eu-LISA.

5. Medlemsstatene og eu-LISA skal samarbeide ved en sikkerhetshendelse.

6. Kommisjonen skal umiddelbart melde alvorlige hendelser til Europaparlamentet og Rådet. Disse rapportene skal være klassifisert som EU RESTRICTED/RESTREINT UE i samsvar med gjeldende sikkerhetsregler.

7. misbruk av opplysninger, skal medlemsstater, Europol og Det europeiske grense- og kystvaktbyrå sikre at det pålegges sanksjoner i samsvar med artikkel 59.

Artikkel 46

Sondring mellom personer med identiske kjennetegn

1. Når det i forbindelse med registrering av en ny melding viser seg at det allerede finnes en melding i SIS om en person med samme identitetsbeskrivelse, skal SIRENE-kontoret innen 12 timer ta kontakt med den innmeldende medlemsstaten via utveksling av utfyllende opplysninger for å kryssjekke om gjenstandene for de to meldingene er samme person.

2. Dersom kryssjekkingen viser at personen i den nye meldingen og personen i meldingen som allerede er registrert i SIS, virkelig er den samme, skal SIRENE-kontoret iverksette framgangsmåten for registrering av flere meldinger i henhold til artikkel 23.

3. Dersom kryssjekkingen viser at det faktisk dreier seg om to forskjellige personer, skal SIRENE-kontoret godkjenne anmodningen om å registrere den andre meldingen ved å tilføye nødvendige opplysninger for å hindre feilidentifisering.

Artikkel 47

Utdypende opplysninger med sikte på å håndtere misbruk av identitet

1. Dersom det kan oppstå forveksling mellom personen som er den tiltenkte gjenstand for en melding, og en person hvis identitet er blitt misbrukt, skal den innmeldende medlemsstaten med uttrykkelig samtykke fra personen hvis identitet er blitt misbrukt, tilføye opplysninger til meldingen om sistnevnte for å unngå de negative konsekvensene av feilidentifisering. Enhver hvis identitet er blitt misbrukt, har rett til å trekke sitt samtykke til behandling av de tilføyde personopplysningene.

2. Opplysninger om en person hvis identitet er blitt misbrukt, skal bare brukes for følgende formål:

(a) for å gjøre det mulig for vedkommende myndighet å sondre mellom personen hvis identitet er blitt misbrukt, og den personen meldingen faktisk gjelder, og

(b) for å gjøre det mulig for personen hvis identitet er blitt misbrukt, å bevise sin identitet og fastslå at vedkommendes identitet er blitt misbrukt.

3. I henhold til denne artikkel og med forbehold for et uttrykkelig samtykke fra personen hvis identitet er blitt misbrukt for hver enkelt kategori av opplysninger, kan bare følgende personopplysninger om en person hvis identitet er blitt misbrukt, registreres og viderebehandles i SIS:

a) etternavn,

b) fornavn,

(c) navn ved fødsel,

(d) tidligere brukte navn og eventuelle særskilt registrerte aliasnavn,

(e) særlige objektive fysiske kjennetegn av uforanderlig art,

(f) fødested,

(g) fødselsdato,

(h) kjønn,

(i) fotografier og ansiktsbilder,

(j) fingeravtrykk, håndflateavtrykk eller begge,

(k) samtlige nasjonaliteter,

(l) arten av personens identitetsdokumenter,

(m) land som har utstedt personens identitetsdokumenter,

(n) nummer/numre på personens identifitetsdokumenter,

(o) dato for utstedelse av en persons identitetsdokumenter,

(p) personens adresse,

(q) personens fars navn,

(r) personens mors navn.

4. Kommisjonen skal vedta gjennomføringsrettsakter for å fastsette og utvikle nødvendige tekniske regler for å registrere og viderebehandle opplysningene nevnt i nr. 3 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

5. Opplysningene omhandlet i nr. 3 skal slettes samtidig som den tilsvarende meldingen, eventuelt tidligere dersom personen anmoder om det.

6. Bare myndigheter som har tilgangsrett til den tilsvarende meldingen, har tilgang til opplysningene omhandlet i nr. 3. De har utelukkende tilgang med sikte på å unngå feilidentifisering.

Artikkel 48

Koplinger mellom meldinger

1. En medlemsstat kan opprette en kopling mellom meldinger den legger inn i SIS. Virkningen av en slik kopling skal være å skape en forbindelse mellom to eller flere meldinger.

2. Opprettelsen av en kopling skal ikke påvirke de særlige tiltakene som skal treffes på grunnlag av hver av de sammenkoplede meldingene, eller meldingenes undersøkelsesfrist.

3. Opprettelsen av en kopling skal ikke påvirke tilgangsrettighetene i henhold til denne forordning. Myndigheter som ikke har tilgang til visse kategorier av meldinger, skal ikke kunne se koplingen til en melding de ikke har tilgang til.

4. En medlemsstat skal opprette en kopling mellom meldinger når det er et klart operativt behov.

5. Dersom en medlemsstat finner at en annen medlemsstats opprettelse av en kopling mellom meldinger er i strid med dens nasjonale rett eller internasjonale forpliktelser, kan den treffe nødvendige tiltak for å sikre at det ikke gis tilgang til koplingen fra dens nasjonale territorium eller for dens myndigheter som befinner seg utenfor dens territorium.

6. Kommisjonen skal vedta gjennomføringsrettsakter for å fastsette og utvikle tekniske regler for sammenkopling av meldinger. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

Artikkel 49

Formålet med og lagringstid for utfyllende opplysninger

1. For å lette utvekslingen av utfyllende opplysninger skal medlemsstatene ved SIRENE-kontoret lagre en henvisning til beslutningene som ligger til grunn for en melding.

2. Personopplysninger som lagres i filer ved SIRENE-kontoret som et resultat av en utveksling av opplysninger, skal lagres bare så lenge det er nødvendig for å oppnå formålene som ligger til grunn for utvekslingen. De skal under alle omstendigheter slettes senest ett år etter at den tilhørende meldingen er slettet fra SIS.

3. Nr. 2 skal ikke berøre en medlemsstats rett til å lagre opplysninger i sine nasjonale filer som vedrører en bestemt melding som medlemsstaten har registrert, eller en melding som har medført tiltak på dens territorium. Hvor lenge slike opplysninger kan lagres i disse filene, er regulert i nasjonal rett.

Artikkel 50

Overføring av personopplysninger til tredjemann

Opplysninger som behandles i SIS, og de tilknyttede utfyllende opplysningene som utveksles i henhold til denne forordning, skal ikke overføres eller gjøres tilgjengelige for tredjestater eller internasjonale organisasjoner.

KAPITTEL IX

VERN AV PERSONOPPLYSNINGER

Artikkel 51

Gjeldende lovgivning

1. Forordning (EU) 2018/1725 får anvendelse på eu-LISAs og Det europeiske grense- og kystvaktbyrås behandling av personopplysninger i henhold til denne forordning. Forordning (EU) 2016/794 får anvendelse på Europols behandling av personopplysninger i henhold til denne forordning.

2. Forordning (EU) 2016/679 får anvendelse på behandling av personopplysninger i henhold til denne forordning foretatt av vedkommende myndigheter nevnt i artikkel 34 i denne forordning med unntak av behandling med sikte på å forebygge, avsløre, etterforske eller rettsforfølge straffbare forhold eller fullbyrde strafferettslige sanksjoner, herunder verne mot og forebygge trusler mot den offentlige sikkerhet, dersom direktiv (EU) 2016/680 kommer til anvendelse.

Artikkel 52

Rett til opplysninger

1. Tredjestatsborgere som omfattes av en melding i SIS, skal underrettes om dette i samsvar med artikkel 13 og 14 i forordning (EU) 2016/679 eller artikkel 12 og 13 i direktiv (EU) 2016/680. Underretningen skal gis skriftlig, sammen med en kopi av eller en henvisning til den nasjonale beslutningen som ligger til grunn for meldingen, som omhandlet i artikkel 24 nr. 1 i denne forordning.

2. Disse opplysningene skal ikke gis dersom nasjonal rett tillater begrenset rett til underretning, særlig for å beskytte statens sikkerhet, forsvaret og den offentlige sikkerhet og forebygge, avsløre, etterforske og rettsforfølge straffbare forhold.

Artikkel 53

Rett til innsyn, retting av uriktige opplysninger og sletting av urettmessig registrerte opplysninger

1. Registrerte skal ha mulighet til å utøve rettighetene fastsatt i artikkel 15, 16 og 17 i forordning (EU) 2016/679 og i artikkel 14 og artikkel 16 nr. 1 og 2 i direktiv (EU) 2016/680.

2. En annen medlemsstat enn den innmeldende medlemsstaten kan gi den registrerte opplysninger om alle de av den registrertes personopplysninger som behandles, bare dersom den på forhånd har gitt den innmeldende medlemsstat mulighet til å uttale seg. Kommunikasjonen mellom disse medlemsstatene skal skje via utveksling av utfyllende opplysninger.

3. En medlemsstat skal i samsvar med nasjonal rett treffe en beslutning om helt eller delvis å unnlate å gi informasjon til den registrerte, dersom og så lenge denne unnlatelsen er et nødvendig og forholdsmessig tiltak i et demokratisk samfunn med nødvendig hensyn til den berørte registrertes grunnleggende rettigheter og berettigede interesser, for å

a) unngå at det legges hindringer i veien for offisielle eller rettslige undersøkelser, etterforskninger eller framgangsmåter,

b) unngå å skade forebygging, avsløring, etterforskning eller rettsforfølging av straffbare forhold eller fullbyrding av strafferettslige sanksjoner,

(c) verne den offentlige sikkerhet,

(d) verne den nasjonale sikkerhet, eller

(e) verne andres rettigheter og friheter.

I saker nevnt i første ledd skal medlemsstaten skriftlig og uten ugrunnet opphold underrette den registrerte om enhver nektet eller begrenset tilgang og om begrunnelsene for nektelsen eller begrensningen. Disse opplysningene kan utelates dersom utleveringen av dem vil være til skade for et av formålene i første ledd bokstav a)–e). Medlemsstaten skal underrette den registrerte om muligheten til å inngå klage til en tilsynsmyndighet eller for rettslig prøving.

Medlemsstaten skal dokumentere de faktiske eller rettslige begrunnelser for beslutningen om ikke å gi opplysninger til den registrerte. Opplysningene skal gjøres tilgjengelige for tilsynsmyndighetene.

I slike tilfeller skal den registrerte også kunne utøve sine rettigheter gjennom vedkommende tilsynsmyndigheter.

4. Etter en søknad om tilgang, retting eller sletting skal medlemsstaten underrette den registrerte så snart som mulig og under alle omstendigheter innen fristene nevnt i artikkel 12 nr. 3 i forordning (EU) 2016/679 om oppfølgingen av utøvelsen av rettighetene i henhold til denne artikkel, uavhengig av om den registrerte befinner seg i en tredjestat eller ikke.

Artikkel 54

Klageadgang

1. Uten at det berører bestemmelsene om klageadgang i forordning (EU) 2016/679 og direktiv (EU) 2016/680, skal enhver kunne få sin sak prøvet av vedkommende myndighet, herunder en domstol, i henhold til retten i den enkelte medlemsstat med sikte på å få innsyn i, rette, slette, få opplysninger om eller søke erstatning i forbindelse med en melding som berører vedkommende.

2. Uten at det berører artikkel 58, forplikter medlemsstatene seg gjensidig til å fullbyrde endelige beslutninger truffet av domstolene eller myndighetene omhandlet i nr. 1 i denne artikkel.

3. Medlemsstatene skal rapportere årlig til Det europeiske personvernråd om

a) antallet anmodninger til den behandlingsansvarlige om tilgang og antallet tilfeller der det ble gitt tilgang til opplysninger,

b) antallet anmodninger til tilsynsmyndigheten om tilgang og antallet tilfeller der det ble gitt tilgang til opplysninger,

(c) antallet anmodninger til den behandlingsansvarlige om retting av uriktige opplysninger og sletting av ulovlig lagrede opplysninger og antallet tilfeller der opplysninger ble rettet eller slettet,

(d) antallet anmodninger til tilsynsmyndigheten om retting av uriktige opplysninger og sletting av ulovlig lagrede opplysninger,

(e) antallet anlagte rettssaker,

(f) antallet saker der domstolen ga søkeren medhold,

(g) eventuell bemerkninger om tilfeller av gjensidig anerkjennelse av endelige beslutninger truffet av domstoler eller myndigheter i andre medlemsstater om meldinger registrert av den innmeldende medlemsstaten.

Kommisjonen utarbeider en mal for rapportering i henhold til dette nummer.

4. Rapportene fra medlemsstatene skal innarbeides i den felles rapporten nevnt i artikkel 57 nr. 4.

Artikkel 55

Tilsyn med N.SIS

1. Medlemsstatene skal sikre at de uavhengige tilsynsmyndighetene som er utpekt i hver medlemsstat, og som har fullmaktene omhandlet i kapittel VI i forordning (EU) 2016/679 eller kapittel VI i direktiv 2016/680, fører kontroll med at behandlingen av personopplysninger i SIS på dens territorium, overføringen av opplysninger fra dens territorium og utvekslingen og den videre behandling av utfyllende opplysninger på dens territorium skjer på lovlig måte.

2. Tilsynsmyndighetene skal sikre at det minst hvert fjerde år gjennomføres en revisjon av behandlingen av opplysninger i N.SIS i samsvar med internasjonale revisjonsstandarder. Revisjonen skal enten utføres av tilsynsmyndighetene, eller tilsynsmyndighetene skal bestille revisjonen direkte hos en uavhengig revisor med ekspertise innenfor personvern. Tilsynsmyndighetene skal til enhver tid bevare kontrollen over og påta seg ansvaret for den uavhengige revisoren.

3. Medlemsstatene skal sikre at deres tilsynsmyndigheter har tilstrekkelige ressurser til å utføre oppgavene som de er tillagt i henhold til denne forordning, og at de har adgang til rådgivning fra personer med tilstrekkelig kunnskap om biometriske opplysninger.

Artikkel 56

Tilsyn med eu-LISA

1. EUs datatilsyn skal være ansvarlig for å føre tilsyn med eu-LISAs behandling av personopplysninger og sikre at behandlingen foretas i samsvar med denne forordning. Oppgavene og fullmaktene fastsatt i artikkel 57 og 58 i forordning (EU) 2018/1725 skal gjelde tilsvarende.

2. EUs datatilsynet skal minst hvert fjerde år gjennomføre en revisjon av eu-LISAs behandling av personopplysninger i samsvar med internasjonale revisjonsstandarder. En rapport om denne revisjonen skal oversendes til Europaparlamentet, til Rådet, til eu-LISA, til Kommisjonen og til tilsynsmyndighetene. eu-LISA skal ha mulighet til å framsette kommentarer før rapporten vedtas.

Artikkel 57

Samarbeid mellom tilsynsmyndigheter og EUs datatilsyn

1. Tilsynsmyndighetene og EUs datatilsyn, hver innenfor sitt kompetanseområde, skal samarbeide aktivt innenfor rammen av sine ansvarsområder og sikre samordnet kontroll med SIS.

2. Tilsynsmyndighetene og EUs datatilsyn skal, hver innenfor sitt kompetanseområde, utveksle relevante opplysninger, bistå hverandre i gjennomføringen av revisjoner og inspeksjoner, utrede vanskeligheter i forbindelse med fortolkningen eller anvendelsen av denne forordning og andre gjeldende unionsrettsakter, undersøke problemer som avdekkes med gjennomføringen av uavhengige kontroller eller med utøvelsen av de registrertes rettigheter, utarbeide harmoniserte forslag til felles løsninger på eventuelle problemer og i påkommende tilfeller fremme bevissthet om personvernrettigheter.

3. Tilsynsmyndighetene og EUs datatilsyn skal møtes i henhold til nr. 2 minst to ganger i året innenfor rammene av Det europeiske personvernråd. Utgifter og tjenester i forbindelse med disse møtene skal dekkes av Det europeiske personvernråd. En forretningsorden skal vedtas på første møte. Øvrige arbeidsmetoder skal utvikles i fellesskap etter behov.

4. EUs datatilsyn skal annethvert år oversende en felles aktivitetsrapport til Europaparlamentet, til Rådet og til Kommisjonen.

KAPITTEL X

ERSTATNINGSANSVAR OG SANKSJONER

Artikkel 58

Erstatningsansvar

1. Uten at det berører retten til erstatning og ethvert erstatningsansvar i henhold til forordning (EU) 2016/679, direktiv (EU) 2016/680 og forordning (EU) 2018/1725

(a) skal enhver person eller medlemsstat som er påført materiell eller immateriell skade som følge av en ulovlig behandling av personopplysninger i forbindelse med bruken av N.SIS eller enhver annen handling fra en medlemsstats side som er i strid med denne forordning, ha rett til erstatning fra nevnte medlemsstat, og

(b) skal enhver person eller medlemsstat som er påført materiell eller immateriell skade som følge av enhver handling fra eu-LISAs side som er i strid med denne forordning, ha rett til erstatning fra eu-LISA.

En medlemsstat eller eu-LISA skal fritas helt eller delvis for erstatningsansvar i henhold til første ledd dersom de beviser at de ikke er ansvarlige for hendelsen som førte til skaden.

2. Dersom en medlemsstats manglende oppfyllelse av sine forpliktelser i henhold til denne forordning forårsaker skade på SIS, skal medlemsstaten holdes ansvarlig for skaden, med mindre og i den grad eu-LISA eller en annen medlemsstat som deltar i SIS, ikke har truffet rimelige tiltak for å hindre skaden i å oppstå eller begrense dens omfang.

3. Erstatningskrav mot en medlemsstat for skade nevnt i nr. 1 og 2 skal reguleres etter nevnte medlemsstats nasjonale rett. Erstatningskrav mot en medlemsstat for skaden nevnt i nr. 1 og 2 skal være omfattet av vilkårene fastsatt i traktatene.

Artikkel 59

Sanksjoner

Medlemsstatene skal påse at misbruk av opplysninger i SIS eller behandling av slike opplysninger eller utveksling av utfyllende opplysninger i strid med denne forordning straffes i samsvar med nasjonal rett.

De fastsatte sanksjonene skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende.

KAPITTEL XI

SLUTTBESTEMMELSER

Artikkel 60

Overvåking og statistikk

1. eu-LISA skal sikre at det er innført framgangsmåter for å overvåke hvordan SIS fungerer i forhold til de mål som er fastsatt for produktivitet, kostnadseffektivitet, sikkerhet og kvalitet på tjenesten.

2. eu-LISA skal ha tilgang til de opplysninger om behandlingsprosessene i det sentrale SIS som er nødvendige for teknisk vedlikehold, rapportering, rapportering av datakvalitet og statistikk.

3. eu-LISA skal utarbeide daglig, månedlig og årlig statistikk over antallet registreringer per meldingskategori både for hver medlemsstat og samlet sett. eu-LISA skal også framlegge årlige rapporter over antall treff per meldingskategori, antall søk i SIS og antall ganger SIS ble brukt til å registrere, ajourføre eller slette en melding, både for hver medlemsstat og samlet sett. Slik statistikk skal inneholde statistikk over utveksling av informasjon i henhold til artikkel 27–31. Den utarbeidede statistikken skal ikke inneholde personopplysninger. Den årlige statistiske rapporten skal offentliggjøres.

4. Medlemsstatene, Europol og Det europeiske grense- og kystvaktbyrå skal framlegge for eu-LISA og Kommisjonen opplysningene de trenger for å utarbeide rapportene omhandlet i nr. 3, 5, 7 og 8.

5. eu-LISA skal framlegge for Europaparlamentet, Rådet, medlemsstatene, Kommisjonen, Europol, Det europeiske grense- og kystvaktbyrå og EUs datatilsyn de statistiske rapporter som eu-LISA utarbeider.

For å kunne overvåke gjennomføringen av unionsrettsakter, herunder i henhold til forordning (EU) nr. 1053/2013, kan Kommisjonen anmode eu-LISA om enten regelmessig eller unntaksvis om å framlegge ytterligere særskilte statistiske rapporter om effektiviteten av SIS, bruken av SIS og utvekslingen av utfyllende opplysninger.

Det europeiske grense- og kystvaktbyrå kan anmode eu-LISA om å framlegge ytterligere særskilte statistiske rapporter med sikte på å foreta risikoanalyser og sårbarhetsvurderinger som nevnt i artikkel 11 og 13 i forordning (EU) 2016/1624, enten regelmessig eller unntaksvis.

6. I henhold til artikkel 15 nr. 4 og nr. 3, 4 og 5 i denne artikkel skal eu-LISA opprette, iverksette og drifte et sentralt datalager i sine tekniske anlegg som inneholder opplysningene nevnt i artikkel 15 nr. 4 og i nr. 3 i denne artikkel, og som ikke skal gjøre det mulig å identifisere enkeltpersoner, og som skal gjøre det mulig for Kommisjonen og byråene nevnt i nr. 5 i denne artikkel å få skreddersydde rapporter og statistikk. eu-LISA skal på anmodning og i det omfang det er nødvendig for å utføre sine oppgaver, gi medlemsstatene, Kommisjonen, Europol og Det europeiske grense- og kystvaktbyrå sikker tilgang til det sentrale register via kommunikasjonsinfrastrukturen. eu-LISA skal gjennomføre tilgangskontroller og særlige brukerprofiler for å sikre at det gis tilgang til det sentrale datalageret utelukkende med sikte på rapportering og statistikk.

7. To år etter at denne forordning er trådt i kraft i henhold til artikkel 66 nr. 5, og deretter annethvert år, skal eu-LISA framlegge for Europaparlamentet og Rådet en rapport om det sentrale SIS' og kommunikasjonsinfrastrukturens tekniske funksjon, herunder dens sikkerhet, om AFIS og om den bilaterale og multilaterale utvekslingen av utfyllende opplysninger mellom medlemsstatene. Denne rapporten skal dessuten, når teknologien er i bruk, inneholde en evaluering av bruken av ansiktsbilder til å identifisere personer.

8. Tre år etter at denne forordning er trådt i kraft i henhold til artikkel 66 nr. 5, og deretter hvert fjerde år, skal Kommisjonen foreta en samlet evaluering av det sentrale SIS og den bilaterale og multilaterale utvekslingen av utfyllende opplysninger mellom medlemsstatene. Den samlede evalueringen skal omfatte en gjennomgang av resultatene som er oppnådd i forhold til målene, og en vurdering av hvorvidt prinsippene som ligger til grunn for systemet, fortsatt er gyldige, av anvendelsen av denne forordning når det gjelder det sentrale SIS, sikkerheten ved det sentrale SIS og eventuelle implikasjoner for framtidige operasjoner. Evalueringsrapporten skal også omfatte en vurdering av AFIS og de SIS-informasjonskampanjer som Kommisjonen gjennomfører i samsvar med artikkel 19.

Evalueringsrapporten skal dessuten inneholde statistikk over antallet meldinger registrert i samsvar med artikkel 24 nr. 1 bokstav a) og statistikk over antallet meldinger registrert i samsvar med bokstav b) i nevnte nummer. Når det gjelder meldinger som er omfattet av artikkel 24 nr. 1 bokstav a), skal det presiseres hvor mange meldinger som ble registrert etter situasjonene nevnt i artikkel 24 nr. 2 bokstav a), b) eller c). Evalueringsrapporten skal dessuten inneholde en vurdering av medlemsstatenes anvendelse av artikkel 24.

Kommisjonen skal oversende evalueringsrapporten til Europaparlamentet og Rådet.

9. Kommisjonen skal vedta gjennomføringsrettsakter om fastsettelse av nærmere regler for drift av det sentrale register nevnt i nr. 6 i denne artikkel og de personvern- og sikkerhetsregler som skal gjelde for dette datalageret. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 62 nr. 2.

Artikkel 61

Utøvelse av delegert myndighet

1. Myndigheten til å vedta delegerte rettsakter gis Kommisjonen på vilkårene fastsatt i denne artikkel.

2. Myndigheten til å vedta de delegerte rettsaktene nevnt i artikkel 33 nr. 4 skal gis Kommisjonen på ubestemt tid fra 27. desember 2018.

3. Den delegerte myndigheten nevnt i artikkel 33 nr. 4 kan når som helst tilbakekalles av Europaparlamentet eller Rådet. Beslutningen om tilbakekalling innebærer at den delegerte myndigheten som angis i beslutningen, opphører å gjelde. Beslutningen trer i kraft dagen etter at den er kunngjort i Den europeiske unions tidende, eller på et senere tidspunkt som er angitt i beslutningen. Den berører ikke gyldigheten av delegerte rettsakter som allerede er trådt i kraft.

4. Før vedtakelsen av en delegert rettsakt skal Kommisjonen rådføre seg med eksperter som er utpekt av hver enkelt medlemsstat i samsvar med prinsippene i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming.

5. Så snart Kommisjonen vedtar en delegert rettsakt, skal den underrette Europaparlamentet og Rådet samtidig om dette.

6. En delegert rettsakt som er vedtatt i henhold til artikkel 33 nr. 4, skal tre i kraft bare dersom verken Europaparlamentet eller Rådet har gjort innsigelse innen to måneder fra den dagen underretning om rettsakten ble gitt Europaparlamentet og Rådet, eller dersom både Europaparlamentet og Rådet før utløpet av denne perioden på to måneder har underrettet Kommisjonen om at de ikke har til hensikt å gjøre innsigelse. Denne perioden skal forlenges med to måneder på initiativ fra Europaparlamentet eller Rådet.

Artikkel 62

Komitéframgangsmåte

1. Kommisjonen skal bistås av en komité. Nevnte komité skal være en komité i henhold til forordning (EU) nr. 182/2011.

2. Når det vises til dette nummer, får artikkel 5 i forordning (EU) nr. 182/2011 anvendelse.

Artikkel 63

Endringer av forordning (EF) nr. 1987/2006

I forordning (EF) nr. 1987/2006 gjøres følgende endringer:

(1) Artikkel 6 skal lyde:

«Artikkel 6

Nasjonale systemer

1. Hver medlemsstat skal ha ansvar for opprettelse, drift, vedlikehold og videreutvikling av sitt eget N.SIS II og for å knytte det til NI-SIS.

2. Hver medlemsstat skal være ansvarlig for å sikre uavbrutt tilgang til SIS II-opplysninger for sluttbrukerne.»

(2) Artikkel 11 skal lyde:

«Artikkel 11

Fortrolighet – medlemsstatene

1. Alle medlemsstater skal anvende egne regler for taushetsplikt eller annen tilsvarende fortrolighetsplikt for alle personer og organer som skal arbeide med SIS II-opplysninger og utfyllende opplysninger, i samsvar med nasjonal rett. Denne plikten skal også gjelde etter at disse personene har sluttet i sin stilling, ansettelsesforholdet er opphørt eller organets virksomhet er avsluttet.

2. Dersom en medlemsstat samarbeider med eksterne leverandører i forbindelse med SIS II-relaterte oppgaver, skal den nøye overvåke leverandørens aktiviteter for å sikre overholdelse av alle bestemmelser i denne forordning, særlig med hensyn til sikkerhet, fortrolighet og personvern.

3. Driftsforvaltningen av N.SIS II eller av tekniske kopier skal ikke overlates til private foretak eller private organisasjoner.»

(3) I artikkel 15 gjøres følgende endringer:

(a) Nytt nummer skal lyde:

«3a. Driftsenheten skal utvikle og opprettholde en mekanisme og framgangsmåter for å utføre kvalitetskontroller av opplysningene i CS-SIS. Det skal regelmessig framlegge rapporter for medlemsstatene i denne forbindelse.

Driftsenheten skal regelmessig framlegge en rapport for Kommisjonen om problemer som har oppstått, og medlemsstater som er berørt.

Kommisjonen skal regelmessig framlegge en rapport for Europaparlamentet og Rådet om problemer som har oppstått med opplysningenes kvalitet.»

(b) Nr. 8 skal lyde:

«8. Driftsforvaltningen av det sentrale SIS skal omfatte alle oppgaver som er nødvendige for å holde det sentrale SIS II i

funksjon 24 timer i døgnet 7 dager i uken i henhold til denne forordning, særlig vedlikeholdsarbeid og tekniske forbedringer som er nødvendig for at systemet skal fungere effektivt. Disse oppgavene skal også omfatte samordning, forvaltning og støtte til utprøvinger for det sentrale SIS II og N.SIS II som sikrer at det sentrale SIS II og N.SIS II fungerer i samsvar med kravene til teknisk og funksjonelt samsvar fastsatt i artikkel 9.»

(4) I artikkel 17 skal nye ledd lyde:

«3. Dersom driftsenheten samarbeider med eksterne leverandører i forbindelse med SIS II-relaterte oppgaver, skal den nøye overvåke leverandørens aktiviteter for å sikre overholdelse av alle bestemmelser i denne forordning, særlig med hensyn til sikkerhet, fortrolighet og personvern.

4. Driftsforvaltningen av CS-SIS skal ikke overlates til private foretak eller private organisasjoner.»

(5) I artikkel 20 nr. 2 innsettes følgende nummer:

«ka) typen straffbart forhold,»

(6) I artikkel 21 skal nytt ledd lyde:

«Dersom beslutningen om nektet innreise og opphold nevnt i artikkel 24 nr. 2 er knyttet til en terrorhandling, skal saken anses for å være adekvat, relevant og viktig nok til at en melding bør registreres i SIS II. Av hensyn til den offentlige eller nasjonale sikkerhet kan medlemsstatene unntaksvis unnlate å registrere en melding når det er sannsynlig at den vil hindre offisielle eller rettslige undersøkelser, etterforskninger eller framgangsmåter.»

(7) Artikkel 22 skal lyde:

«Artikkel 22

Særlige regler for registrering eller kontroll av eller søk med fotografier og fingeravtrykk

1. Fotografier og fingeravtrykk skal bare registreres etter en særlig kvalitetskontroll for å kontrollere om opplysningene oppfyller en minste kvalitetsstandard. Spesifikasjonene for den særlige kvalitetskontrollen skal fastsettes i samsvar med framgangsmåten omhandlet i artikkel 51 nr. 2.

2. Når en melding i SIS inneholder fotografier, ansiktsbilder og fingeravtrykksopplysninger, skal slike fotografier, ansiktsbilder og fingeravtrykksopplysninger brukes til å bekrefte identiteten til en person som er funnet som følge av et alfanumerisk søk i SIS.

3. Det kan i alle tilfeller søkes på fingeravtrykksopplysninger for å identifisere en person. Det skal imidlertid søkes på fingeravtrykksopplysninger for å identifisere en person dersom en persons identitet ikke kan fastslås på annen måte. For det formål skal det sentrale SIS II inneholde et system for automatisert fingeravtrykksidentifisering (AFIS).

4. Det kan også søkes på fingeravtrykksopplysninger i SIS i forbindelse med meldinger som er registrert i samsvar med artikkel 24 og 26, ved bruk av fullstendige eller ufullstendige sett av fingeravtrykk eller håndflateavtrykk som er funnet på et åsted under etterforskning av grov kriminalitet eller terrorhandlinger, dersom det med stor sannsynlighet kan fastslås at disse settene av avtrykk tilhører en gjerningsperson, og forutsatt at søket foretas samtidig i medlemsstatens relevante nasjonale fingeravtrykksdatabaser.»

(8) Artikkel 26 skal lyde:

«Artikkel 26

Vilkår for registrering av meldinger om tredjestatsborgere som er omfattet av restriktive tiltak

1. Meldinger om tredjestatsborgere som omfattes av restriktive tiltak for å hindre innreise til eller transitt gjennom medlemsstatenes territorium, truffet i henhold til rettsakter vedtatt av Rådet, herunder tiltak for å gjennomføre reiseforbud utstedt av De forente nasjoners sikkerhetsråd, skal registreres i SIS II for å nekte innreise eller opphold, forutsatt at kravene til opplysningenes kvalitet er oppfylt.

2. Meldingene skal registreres, ajourføres og slettes av vedkommende myndighet i medlemsstaten som har formannskapet for Rådet for Den europeiske union på tidspunktet tiltaket vedtas. Dersom denne medlemsstaten ikke har tilgang til SIS II eller til meldinger registrert i samsvar med denne forordning, skal ansvaret påhvile medlemsstaten som har formannskapet i den påfølgende perioden, og som har tilgang til SIS II, herunder meldinger registrert i samsvar med denne forordning.

Medlemsstatene skal innføre nødvendige framgangsmåter for å registrere, ajourføre og slette slike meldinger.

(9) Nye artikler skal lyde:

«Artikkel 27a

Europols tilgang til opplysninger i SIS II

1. Den europeiske unions byrå for politisamarbeid (Europol), opprettet ved europaparlaments- og rådsforordning (EU) 2016/794, skal, dersom det er nødvendig for at Europol skal oppfylle sitt mandat, ha tilgangsrett til og rett til å søke i opplysninger i SIS II. Europol kan også utveksle og anmode om utfyllende opplysninger i samsvar med bestemmelsene i SIRENE-håndboken.

2. Dersom et søk foretatt av Europol viser at det finnes en melding i SIS II, skal Europol underrette den innmeldende medlemsstaten via utveksling av utfyllende opplysninger ved hjelp av kommunikasjonsinfrastrukturen og i samsvar med bestemmelsene i SIRENE-håndboken. Inntil Europol kan bruke funksjonene for utveksling av utfyllende opplysninger, skal Europol underrette den innmeldende medlemsstaten via kanalene fastsatt i forordning (EU) 2016/794.

3. Europol kan behandle de utfyllende opplysningene som er oversendt fra medlemsstater for å sammenligne dem med sine databaser og prosjekter for operative analyser som skal finne sammenhenger eller andre relevante koplinger, og for analyser av strategisk, tematisk eller operativ art som nevnt i artikkel 18 nr. 2 bokstav a), b) og c) i forordning (EU) 2016/794. Enhver behandling av utfyllende opplysninger foretatt av Europol i henhold til denne artikkel skal utføres i samsvar med nevnte forordning.

4. Europols bruk av opplysninger fra søk i SIS II eller fra behandling av utfyllende opplysninger skal kreve den innmeldende medlemsstatens samtykke. Dersom medlemsstaten tillater at slike opplysninger brukes, skal Europols behandling av dem skje i samsvar med forordning (EU) 2016/794. Europol skal underrette tredjestater og tredjeorganer om slike opplysninger bare med den innmeldende medlemsstatens samtykke og i fullt samsvar med unionsretten om personvern.

5. Europol skal

(a) uten at det berører nr. 4 og 6, ikke kople deler av SIS II til, eller overføre de opplysninger i SIS II som Europol har tilgang til, til noe system for innsamling og behandling av opplysninger drevet av eller ved Europol, eller laste ned eller på annen måte kopiere deler av SIS II,

(b) uten hensyn til artikkel 31 nr. 1 i forordning (EU) 2016/794 slette utfyllende opplysninger som inneholder personopplysninger senest ett år etter at den tilhørende meldingen er slettet. Som et unntak kan Europol, dersom Europol har opplysninger i sine databaser eller prosjekter for operative analyser om en sak med tilknytning til de utfyllende opplysningene, for å kunne utføre sine oppgaver unntaksvis fortsatt lagre de utfyllende opplysningene dersom det er nødvendig. Europol skal underrette den innmeldende og fullbyrdende medlemsstaten om den fortsatte lagring av slike utfyllende opplysninger og begrunne dette,

(c) begrense tilgangen til opplysninger i SIS II, herunder utfyllende opplysninger, til Europol-personale med særskilt fullmakt som har bruk for tilgang til slike opplysninger for å kunne utføre sine oppgaver,

(d) vedta og anvende tiltak for å ivareta sikkerheten, fortroligheten og egenkontrollen i samsvar med artikkel 10, 11 tilog 13,

(e) sikre at personale med fullmakt til å behandle SIS UU-opplysninger får relevant opplæring og informasjon i samsvar med artikkel 14, og

(f) uten at det berører forordning (EU) 2016/794, la EUs datatilsyn overvåke og undersøke Europols aktiviteter når det utøver sin tilgangsrett og rett til å søke i opplysninger i SIS II og utveksle og behandle utfyllende opplysninger.

6. Europol skal kopiere opplysninger fra SIS II bare for tekniske formål, dersom dette er nødvendig for at Europol-personale med tilstrekkelig fullmakt kan foreta et direkte søk. Denne forordning skal også gjelde slike kopier. Den tekniske kopien skal brukes bare for å lagre SIS II-opplysninger mens det søkes i disse opplysningene. Når det er søkt i opplysningene, skal de slettes. Slik bruk skal ikke anses som ulovlig nedlasting eller kopiering av SIS II-opplysninger. Europol skal ikke kopiere meldingsopplysninger eller tilleggsopplysninger fra medlemsstater eller CS-SIS II til andre Europol-systemer.

7. Europol skal i samsvar med bestemmelsene i artikkel 12 føre logger over hver tilgang til og hvert søk i SIS II for å kontrollere om behandlingen av opplysninger skjer på lovlig vis, utøve egenkontroll og ivareta opplysningers sikkerhet og integritet. Disse loggene og denne dokumentasjonen skal ikke anses som ulovlig nedlasting eller kopiering fra en del av SIS II.

8. Medlemsstatene skal underrette Europol via utveksling av utfyllende opplysninger om eventuelle treff på meldinger i forbindelse med terrorhandlinger. Medlemsstatene kan unntaksvis unnlate å underrette Europol dersom dette ville sette igangværende etterforskninger eller en fysisk persons sikkerhet i fare eller være i strid med vesentlige sikkerhetsinteresser i den innmeldende medlemsstaten.

9. Nr. 8 får anvendelse fra den dato Europol kan motta utfyllende opplysninger i samsvar med nr. 1.

Artikkel 27b

Tilgang til opplysninger i SIS II for europeiske grense- og kystvaktenheter, enheter med personale som arbeider med tilbakesendingsrelaterte oppgaver, og medlemmene av støttegruppene for migrasjonsstyring

1. I samsvar med artikkel 40 nr. 8 i europaparlaments- og rådsforordning (EU) 2016/1624 (**) skal medlemmene i enhetene nevnt i artikkel 2 nr. 8 og 9 i nevnte forordning i sitt mandat, og forutsatt at de har tillatelse til å foreta kontroller i henhold til artikkel 27 nr. 1 i denne forordning og har fått nødvendig opplæring i henhold til artikkel 14 i denne forordning, ha tilgangsrett og rett til søk i opplysninger i SIS II dersom det er nødvendig for at de skal kunne utføre sin oppgave, og i den grad det kreves i henhold til driftsplanen for en spesifikk operasjon. Tilgang til opplysninger i SIS II skal ikke utvides til andre medlemmer i enheten.

2. Medlemmene i enhetene nevnt i nr. 1 skal utøve tilgangsretten og retten til å søke i opplysninger i SIS II i samsvar med nr. 1 via et teknisk grensesnitt. Det tekniske grensesnittet skal opprettes og vedlikeholdes av Det europeiske grense- og kystvaktbyrå og skal sikre en direkte forbindelse til det sentrale SIS II.

3. Når et søk foretatt av et medlem i enhetene nevnt i nr. 1 i denne artikkel viser at det foreligger en melding i SIS II, skal den innmeldende medlemsstaten underrettes om dette. I samsvar med artikkel 40 i forordning (EU) 2016/1624 skal medlemmer i enhetene bare reagere på en melding i SIS II i henhold til instruksene fra og som hovedregel i nærvær av grensevakter eller personale som arbeider med tilbakesending i vertsmedlemsstaten der de opererer. Vertsmedlemsstaten kan gi medlemmene av enhetene tillatelse til å handle på dens vegne.

4. Det europeiske grense- og kystvaktbyrå skal i samsvar med bestemmelsene i artikkel 12 føre logger over hver tilgang til og hvert søk i SIS II for å kontrollere om behandlingen av opplysninger skjer på lovlig vis, utøve egenkontroll og ivareta opplysningers sikkerhet og integritet.

5. Det europeiske grense- og kystvaktbyrå skal vedta og anvende tiltak for å ivareta sikkerheten, fortroligheten og egenkontrollen i samsvar med artikkel 10, 11 og 13 og skal sikre at enhetene nevnt i nr. 1 i denne artikkel anvender disse tiltakene.

6. Ingenting i denne artikkel skal forstås slik at det berører bestemmelsene i forordning (EU) 2016/1624 om vern av personopplysninger eller Det europeiske grense- og kystvaktbyrås ansvar for sin uautoriserte eller uriktige behandling av opplysninger.

7. Uten at det berører nr. 2, skal ingen deler av SIS II koples til noe system for innsamling eller behandling av opplysninger som drives av enhetene nevnt i nr. 1 eller av Det europeiske grense- og kystvaktbyrå, og heller ikke skal opplysningene i SIS II som enhetene har tilgang til, overføres til et slikt system. Ingen del av SIS II skal lastes ned eller kopieres. Loggføringen av tilgang og søk skal ikke anses som ulovlig nedlasting eller kopiering av SIS II-opplysninger.

8. Det europeiske grense- og kystvaktbyrå skal tillate at EUs datatilsyn overvåker og undersøker virksomheten til enhetene nevnt i denne artikkel når de utøver sin tilgangsrett og rett til å søke i opplysninger i SIS II. Dette skal ikke berøre de ytterligere bestemmelsene i europaparlaments- og rådsforordning (EU) 2018/1725 (***).

(*) Europaparlaments- og rådsforordning (EU) 2016/794 av 11. mai 2016 om Den europeiske unions byrå for politisamarbeid (Europol) og erstatning og oppheving av rådsbeslutning 2009/371/JIS, 2009/934/JIS, 2009/935/JIS, 2009/936/JIS og 2009/968/JIS (EUT L 135 av 24.5.2016, s. 53)

(**) Europaparlaments- og rådsforordning (EU) 2016/1624 av 14. september 2016 om den europeiske grense- og kystvakt og om endring av europaparlaments- og rådsforordning (EU) 2016/399 og om oppheving av europaparlaments- og rådsforordning (EF) nr. 863/2007, rådsforordning (EF) nr. 2007/2004 og rådsvedtak 2005/267/EF (EUT L 251 av 16.9.2016, s. 1).

(***) Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger og om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

Artikkel 64

Endring av konvensjonen om gjennomføring av Schengen-avtalen

Artikkel 25 i konvensjonen om gjennomføring av Schengen-avtalen utgår.

Artikkel 65

Oppheving

Forordning (EF) nr. 1987/2006 oppheves fra den dato denne forordning får anvendelse som fastsatt i artikkel 66 nr. 5 første ledd.

Henvisninger til den opphevede forordningen skal forstås som henvisninger til denne forordning og leses som angitt i sammenligningstabellen i vedlegget.

Artikkel 66

Ikrafttredelse, driftsstart og anvendelse

1. Denne forordning trer i kraft den 20. dag etter at den er kunngjort i Den europeiske unions tidende.

2. Kommisjonen skal innen 28. desember 2021 vedta en beslutning om fastsettelse av datoen for når SIS settes i drift i henhold til denne forordning etter kontroll av at følgende vilkår er oppfylt:

a) Gjennomføringsrettsaktene som er nødvendige for å anvende denne forordning, er blitt vedtatt.

b) Medlemsstater har underrettet Kommisjonen om at de har gjennomført de tekniske og lovmessige tiltak som er nødvendige for å kunne behandle opplysninger i SIS og utveksle utfyllende opplysninger i henhold til denne forordning.

(c) eu-LISA har underrettet Kommisjonen om at alle utprøvinger i forbindelse med CS-SIS og samspillet mellom CS-SIS og N.SIS er avslutttet på tilfredsstillende måte.

3. Kommisjonen skal nøye overvåke prosessen med gradvis oppfyllelse av vilkårene i nr. 2 og skal underrette Europaparlamentet og Rådet om resultatet av kontrollen omhandlet i nevnte nummer.

4. Kommisjonen skal innen 28. desember 2019 og deretter hvert år til Kommisjonen har truffet beslutningen nevnt i nr. 2, framlegge for Europaparlamentet og Rådet en rapport om status med hensyn til forberedelsen av den fullstendige gjennomføring av denne forordning. Denne rapporten skal også inneholde nærmere opplysninger om de påløpte utgiftene og opplysninger om eventuell risiko som kan ha innvirkning på de samlede kostnader.

5. Denne forordning får anvendelse fra den dato som fastsettes i samsvar med nr. 2.

Som unntak fra første ledd

a) får artikkel 4 nr. 4, artikkel 5, artikkel 8 nr. 4, artikkel 9 nr. 1 og 5, artikkel 15 nr. 7, artikkel 19, artikkel 20 nr. 3 og 4, artikkel 32 nr. 4, artikkel 33 nr. 4, artikkel 47 nr. 4, artikkel 48 nr. 6, artikkel 60 nr. 6 og 9, artikkel 61, artikkel 62, artikkel 63 nr. 1–6 og 8 og nr. 3 og 4 i denne artikkel anvendelse fra datoen for ikrafttredelse av denne forordning,

får artikkel 63 nr. 9 bokstav b) anvendelse fra 28. desember 2019,

(c) får artikkel 63 punkt 7 anvendelse fra 28. desember 2020.

6. Kommisjonsbeslutningen nevnt i nr. 2 skal offentliggjøres i Den europeiske unions tidende.

Denne forordning er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater i samsvar med traktatene.

Utferdiget i Brussel, 28. november 2018.

For Europaparlamentet
President
A. TAJANI

For Rådet
Formann
K. EDTSTADLER

VEDLEGG

SAMMENLIGNINGSTABELL

Forordning (EF) nr. 1987/2006	Denne forordning
Artikkel 1	Artikkel 1
Artikkel 2	Artikkel 2
Artikkel 3	Artikkel 3
Artikkel 4	Artikkel 4
Artikkel 5	Artikkel 5
Artikkel 6	Artikkel 6
Artikkel 7	Artikkel 7
Artikkel 8	Artikkel 8
Artikkel 9	Artikkel 9
Artikkel 10	Artikkel 10
Artikkel 11	Artikkel 11
Artikkel 12	Artikkel 12
Artikkel 13	Artikkel 13
Artikkel 14	Artikkel 14
Artikkel 15	Artikkel 15
Artikkel 16	Artikkel 16
Artikkel 17	Artikkel 17
Artikkel 18	Artikkel 18
Artikkel 19	Artikkel 19
Artikkel 20	Artikkel 20
Artikkel 21	Artikkel 21
Artikkel 22	Artikkel 32 og 33
Artikkel 23	Artikkel 22
–	Artikkel 23
Artikkel 24	Artikkel 24
Artikkel 25	Artikkel 26
Artikkel 26	Artikkel 25
–	Artikkel 27
–	Artikkel 28
–	Artikkel 29
–	Artikkel 30
–	Artikkel 31
Artikkel 27	Artikkel 34
Artikkel 27a	Artikkel 35
Artikkel 27b	Artikkel 36
–	Artikkel 37
Artikkel 28	Artikkel 38
Artikkel 29	Artikkel 39
Artikkel 30	Artikkel 40
Artikkel 31	Artikkel 41

Forordning (EF) nr. 1987/2006	Denne forordning
Artikkel 32	Artikkel 42
Artikkel 33	Artikkel 43
Artikkel 34	Artikkel 44
–	Artikkel 45
Artikkel 35	Artikkel 46
Artikkel 36	Artikkel 47
Artikkel 37	Artikkel 48
Artikkel 38	Artikkel 49
Artikkel 39	Artikkel 50
Artikkel 40	–
–	Artikkel 51
Artikkel 41	Artikkel 53
Artikkel 42	Artikkel 52
Artikkel 43	Artikkel 54
Artikkel 44	Artikkel 55
Artikkel 45	Artikkel 56
Artikkel 46	Artikkel 57
Artikkel 47	–
Artikkel 48	Artikkel 58
Artikkel 49	Artikkel 59
Artikkel 50	Artikkel 60
–	Artikkel 61
Artikkel 51	Artikkel 62
Artikkel 52	–
–	Artikkel 63
–	Artikkel 64
Artikkel 53	–
–	Artikkel 65
Artikkel 54	–
Artikkel 55	Artikkel 66