DEN EUROPÆISKE UNION

EUROPA-PARLAMENTET **RÅDET**

Bruxelles, den 28. november 2018
(OR. en)

2016/0408 (COD)
LEX 1848

PE-CONS 35/1/18
REV 1

SIRIS 70
FRONT 189
SCHENGEN 29
COMIX 334
CODEC 1125

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING OM OPRETTELSE, DRIFT OG BRUG AF SCHENGENINFORMATIONSSYSTEMET (SIS) PÅ OMRÅDET IND- OG UDREJSEKONTROL, OM ÆNDRING AF KONVENTIONEN OM GENNEMFØRELSE AF SCHENGENAFTALEN OG OM ÆNDRING OG OPHÆVELSE AF FORORDNING (EF) NR. 1987/2006

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2018/...

af 28. november 2018

om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området ind- og udrejsekontrol, om ændring af konventionen om gennemførelse af Schengenaftalen og om ændring og ophævelse af forordning (EF) nr. 1987/2006

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 77, stk. 2, litra b) og d), og artikel 79, stk. 2, litra c),

under henvisning til forslag fra Europa-Kommissionen,

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

efter den almindelige lovgivningsprocedure[1], og

ud fra følgende betragtninger:

[1] Europa-Parlamentets holdning af 24.10.2018 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 19.11.2018.

(1) Schengeninformationssystemet (SIS) udgør et væsentligt redskab for anvendelsen af bestemmelserne i Schengenreglerne som integreret i Den Europæiske Union. SIS er en af de vigtigste kompenserende foranstaltninger, der bidrager til at opretholde et højt sikkerhedsniveau inden for Unionens område med frihed, sikkerhed og retfærdighed ved at støtte det operationelle samarbejde mellem nationale kompetente myndigheder, navnlig grænsevagter, politiet, toldmyndigheder, immigrationsmyndigheder og myndigheder med ansvar for at forebygge, afsløre, efterforske eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner.

(2) SIS blev oprindelig oprettet i medfør af bestemmelserne i afsnit IV i konventionen af 19. juni 1990 om gennemførelse af Schengenaftalen af 14. juni 1985 mellem regeringerne for staterne i Den Økonomiske Union Benelux, Forbundsrepublikken Tyskland og Den Franske Republik om gradvis ophævelse af kontrollen ved de fælles grænser[1] (Schengengennemførelseskonventionen). Kommissionen fik til opgave at udvikle anden generation af SIS (SIS II) i henhold til Rådets forordning (EF) nr. 2424/2001[2] og Rådets afgørelse 2001/886/RIA[3]. Det blev senere oprettet ved Europa-Parlamentets og Rådets forordning (EF) nr. 1987/2006[4] og Rådets afgørelse 2007/533/RIA[5]. SIS II erstattede det ved Schengengennemførelseskonventionen indførte SIS.

---

1 EUT L 239 af 22.9.2000, s. 19.

2 Rådets forordning (EF) nr. 2424/2001 af 6. december 2001 om udviklingen af anden generation af Schengeninformationssystemet (SIS II) (EFT L 328 af 13.12.2001, s. 4).

3 Rådets afgørelse 2001/886/RIA af 6. december 2001 om udviklingen af anden generation af Schengeninformationssystemet (SIS II) (EFT L 328 af 13.12.2001, s. 1).

4 Europa-Parlamentets og Rådets forordning (EF) nr. 1987/2006 af 20. december 2006 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 381 af 28.12.2006, s. 4).

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

(3) Tre år efter idriftsættelsen af SIS II foretog Kommissionen en evaluering af systemet i overensstemmelse med forordning (EF) nr. 1987/2006 og afgørelse 2007/533/RIA. Den 21. december 2016 forelagde Kommissionen Europa-Parlamentet og Rådet rapporten om evalueringen af anden generation af Schengeninformationssystemet (SIS II) i overensstemmelse med artikel 24, stk. 5, artikel 43, stk. 3, og artikel 50, stk. 5, i forordning (EF) nr. 1987/2006 samt artikel 59, stk. 3, og artikel 66, stk. 5, i afgørelse 2007/533/RIA og et ledsagende arbejdsdokument. Anbefalingerne i disse dokumenter bør afspejles i nærværende forordning, når det er relevant.

(4) Denne forordning udgør retsgrundlaget for SIS for så vidt angår forhold, der er omfattet af anvendelsesområdet for tredje del, afsnit V, kapitel 2, i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Europa-Parlamentets og Rådets forordning (EU) 2018/…[1+] udgør retsgrundlag for SIS for så vidt angår forhold, der er omfattet af anvendelsesområdet for tredje del, afsnit V, kapitel 4 og 5, i TEUF.

---

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

[+] EUT: Indsæt venligst nummer i teksten og publikationsreference i fodnoten på forordningen i PE-CONS 36/18.

(5) Det forhold, at retsgrundlaget for SIS består af særskilte instrumenter, berører ikke princippet om, at SIS udgør ét enkelt informationssystem, der bør fungere som sådant. Det bør omfatte et enkelt netværk af nationale kontorer, der betegnes SIRENE-kontorerne, til sikring af udveksling af supplerende oplysninger. Visse bestemmelser i disse instrumenter bør derfor være identiske.

(6) Det er nødvendigt at specificere målene for SIS, visse elementer af systemets tekniske arkitektur og dets finansiering, at fastsætte bestemmelser vedrørende "end-to-end"-driften og -brugen af systemet samt at fastlægge ansvarsfordelingen. Det er også nødvendigt at fastlægge de kategorier af oplysninger, der skal indlæses i systemet, formålene med indlæsningen og behandlingen af disse oplysninger og kriterierne for indlæsningen af dem. Regler er også nødvendige for at regulere sletning af indberetninger, de myndigheder, der har adgang til oplysningerne, brugen af biometriske data og for at fastlægge nærmere bestemmelser om databeskyttelse og databehandling.

(7) Indberetninger i SIS indeholder kun de oplysninger, der er nødvendige til at identificere en person og for de handlinger, der skal foretages. Medlemsstaterne bør derfor udveksle supplerende oplysninger i forbindelse med indberetninger, hvor det er påkrævet.

(8) SIS omfatter et centralt system (det centrale SIS) og nationale systemer. De nationale systemer kan indeholde en fuldstændig eller delvis kopi af SIS-databasen, som to eller flere medlemsstater kan være fælles om. Da SIS er det vigtigste instrument til udveksling af oplysninger i Europa med henblik på at garantere sikkerhed og effektiv grænsestyring, er det nødvendigt at sikre en uafbrudt drift af systemet på både centralt og nationalt plan. SIS' tilgængelighed bør være underlagt tæt overvågning på centralt plan og medlemsstatsplan, og ethvert tilfælde af manglende tilgængelighed for slutbrugerne bør registreres og indberettes til de interesserede parter på nationalt plan og EU-plan. Hver enkelt medlemsstat bør foretage backup af sit nationale system. Medlemsstaterne bør også sikre uafbrudt konnektivitet med det centrale SIS ved hjælp af duplikerede og fysisk og geografisk adskilte forbindelsespunkter. Det centrale SIS og kommunikationsinfrastrukturen bør drives, så det sikres, at de fungerer døgnet rundt alle ugens dage. Derfor bør Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed ("eu-LISA"), som er oprettet ved forordning (EU) 2018/…[1+], gennemføre tekniske løsninger for at styrke uafbrudt adgang til SIS, med forbehold af en uafhængig konsekvensanalyse og cost-benefit-analyse.

---

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

[+] EUT: Indsæt venligst nummer i teksten og publikationsreference i fodnoten på forordningen i PE-CONS 29/18.

(9) Det er nødvendigt at have en ajourført håndbog med detaljerede regler om udvekslingen af supplerende oplysninger om de handlinger, der skal foretages som følge af indberetningerne ("SIRENE-håndbogen"). SIRENE-kontorerne bør sikre, at udvekslingen af sådanne oplysninger sker hurtigt og effektivt.

(10) For løbende at sikre en effektiv udveksling af supplerende oplysninger, herunder om de handlinger, der ifølge indberetningerne skal foretages, er det hensigtsmæssigt at styrke SIRENE-kontorernes funktion ved at specificere kravene med hensyn til de disponible ressourcer og brugeruddannelse og svartiden ved forespørgsler fra andre SIRENE-kontorer.

(11) Medlemsstaterne bør sikre, at personalet i deres SIRENE-kontorer har de sproglige færdigheder og det kendskab til relevant ret og proceduremæssige regler, der er nødvendigt for at varetage deres opgaver.

(12) For at være i stand til fuldt ud at nyde gavn af SIS' funktioner bør medlemsstaterne sikre, at SIRENE-kontorernes slutbrugere og personale regelmæssigt modtager uddannelse, herunder i datasikkerhed, databeskyttelse og datakvalitet. SIRENE-kontorerne bør inddrages i arbejdet med at udvikle uddannelsesprogrammer. SIRENE-kontorerne bør så vidt muligt også foretage udveksling af personale med andre SIRENE-kontorer mindst én gang om året. Medlemsstaterne tilskyndes til at træffe passende foranstaltninger for at undgå tab af kvalifikationer og erfaring i forbindelse med personaleomsætning.

(13) Den operationelle forvaltning af de centrale dele af SIS forestås af eu-LISA. For at gøre det muligt for eu-LISA at afsætte de fornødne økonomiske og personalemæssige ressourcer til at dække alle aspekter af den operationelle forvaltning af det centrale SIS og kommunikationsinfrastrukturen bør dets opgaver fastsættes nærmere i denne forordning, navnlig hvad angår de tekniske aspekter ved udvekslingen af supplerende oplysninger.

(14) Uden at det berører medlemsstaternes ansvar for, at de oplysninger, der indlæses i SIS, er korrekte, og SIRENE-kontorernes rolle som kvalitetskoordinatorer, bør eu-LISA være ansvarligt for at højne datakvaliteten ved at indføre et centralt redskab til overvågning af datakvaliteten og bør jævnligt forelægge Kommissionen og medlemsstaterne rapporter. Kommissionen bør aflægge rapport for Europa-Parlamentet og Rådet vedrørende de konstaterede datakvalitetsproblemer. For yderligere at forbedre kvaliteten af oplysningerne i SIS bør eu-LISA også tilbyde uddannelse i brugen af SIS til de nationale uddannelsesinstitutioner og, så vidt muligt, SIRENE-kontorerne og slutbrugerne.

(15) For at muliggøre en bedre overvågning af brugen af SIS til at analysere tendenser vedrørende migrationspres og grænsestyring bør eu-LISA kunne udvikle midler svarende til det aktuelle tekniske niveau til statistisk rapportering til medlemsstaterne, Europa-Parlamentet, Rådet, Kommissionen, Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning uden at bringe dataintegriteten i fare. Der bør derfor oprettes et centralt register. Statistikker, der opbevares i eller indhentes fra nævnte register, bør ikke indeholde personoplysninger. Medlemsstaterne bør fremsende statistikker vedrørende udøvelse af retten til adgang, berigtigelse af ukorrekte oplysninger og sletning af ulovligt lagrede oplysninger inden for rammerne af samarbejde mellem tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse i medfør af denne forordning.

(16) Der bør indføres nye datakategorier i SIS for at gøre det muligt for slutbrugerne at træffe velfunderede afgørelser på grundlag af en indberetning uden at miste tid. Derfor bør indberetninger om nægtelse af indrejse og ophold indeholde oplysninger om den afgørelse, som indberetningen er baseret på. For at lette identifikationen af personer og afsløre personer med flere identiteter bør indberetningen desuden, hvis sådanne oplysninger foreligger, indeholde en henvisning til den berørte persons personlige identitetsdokument eller dets nummer og en kopi af dokumentet, så vidt muligt en farvekopi.

(17) De kompetente myndigheder bør, hvis det er strengt nødvendigt, kunne indlæse specifikke oplysninger i SIS om en persons eventuelle særlige fysiske kendetegn af objektiv og blivende karakter, såsom tatoveringer, mærker eller ar.

(18) Når der oprettes en indberetning, bør alle relevante oplysninger, navnlig den berørte persons fornavn, angives, hvis de er til rådighed, for at minimere risikoen for falske hit og unødige driftsaktiviteter.

(19) SIS bør ikke lagre nogen oplysninger, der anvendes til at foretage søgninger, med undtagelse af logfiler for at kontrollere, hvorvidt søgningen er lovlig, for at overvåge databehandlingens lovlighed, til egenkontrol og for at sikre, at de nationale systemer fungerer korrekt, samt med henblik på dataintegritet og -sikkerhed.

(20) SIS bør gøre det muligt at behandle biometriske data for at sikre en pålidelig identifikation af de pågældende personer. Indlæsning af fotografier, ansigtsbilleder eller fingeraftryksoplysninger i SIS og enhver anvendelse af sådanne oplysninger bør være begrænset til, hvad der er nødvendigt for at nå de tilsigtede mål, bør være tilladt i henhold til EU-retten, bør overholde de grundlæggende rettigheder, herunder barnets tarv, og bør være i overensstemmelse med EU-retten om databeskyttelse, herunder de relevante bestemmelser om databeskyttelse, der er fastsat i denne forordning. For at undgå ubehageligheder på grund af fejlidentifikation bør SIS af samme grund også gøre det muligt at behandle oplysninger vedrørende personer, hvis identitet er blevet misbrugt, med forbehold af passende sikkerhedsforanstaltninger, indhentning af den berørte persons samtykke for hver enkelt datakategori, navnlig håndfladeaftryk, og strenge begrænsninger af de formål, hvortil sådanne personoplysninger lovligt kan behandles.

(21) Medlemsstaterne bør træffe de nødvendige tekniske foranstaltninger for at sikre, at slutbrugere, hver gang de har ret til at foretage en søgning i en af de nationale politi- eller immigrationsmyndigheders databaser, samtidig også søger i SIS, med forbehold af de principper, der er fastsat i artikel 4 i Europa-Parlamentets og Rådets direktiv (EU) 2016/680[1] og artikel 5 i Europa-Parlamentets og Rådets forordning (EU) 2016/679[2]. Dette bør sikre, at SIS fungerer som den vigtigste kompenserende foranstaltning inden for området uden kontrol ved de indre grænser og i højere grad bidrager til at bekæmpe den grænseoverskridende dimension af kriminalitet og kriminelles mobilitet.

(22) Denne forordning bør fastsætte betingelserne for anvendelsen af fingeraftryksoplysninger, fotografier og ansigtsbilleder med henblik på identifikation og verifikation. Ansigtsbilleder og fotografier med henblik på identifikation bør i første omgang kun anvendes ved almindelige grænseovergangssteder. Sådan anvendelse bør gøres til genstand for en rapport fra Kommissionen, hvori det bekræftes, at teknologien er tilgængelig, pålidelig og umiddelbart anvendelig.

---

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

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

(23) Det bør være tilladt at søge på fingeraftryksoplysninger i SIS med fuldstændige eller ufuldstændige sæt af fingeraftryk eller håndfladeaftryk, der er fundet på et gerningssted, hvis det med en høj grad af sandsynlighed kan fastslås, at de tilhører en gerningsmand til grov kriminalitet eller en terrorhandling, såfremt en søgning foretages samtidigt i de relevante nationale fingeraftryksdatabaser. Der bør lægges særlig vægt på fastlæggelse af kvalitetsstandarder for lagring af biometriske data.

(24) Hvis en persons identitet ikke kan fastslås på anden måde, bør fingeraftryksoplysninger anvendes for at forsøge at fastslå identiteten. Det bør i alle tilfælde være tilladt at identificere en person ved hjælp af fingeraftryksoplysninger.

(25) Det bør være muligt for medlemsstaterne at sammenkoble indberetninger i SIS. Det forhold, at to eller flere indberetninger sammenkobles, bør ikke have indflydelse på de handlinger, der skal foretages, undersøgelsesfristen for indberetninger eller adgangen til indberetningerne.

(26) Der kan opnås øget effektivitet, harmonisering og sammenhæng ved at gøre det obligatorisk at indlæse alle de indrejseforbud, der udstedes af nationale kompetente myndigheder, i SIS i overensstemmelse med procedurer, der overholder Europa-Parlamentets og Rådets direktiv 2008/115/EF[1], og ved at fastsætte fælles regler for indlæsning af indberetninger om nægtelse af indrejse og ophold ved tilbagesendelse af en tredjelandsstatsborger med ulovligt ophold. Medlemsstaterne bør træffe alle nødvendige foranstaltninger for at forhindre forsinkelser fra det øjeblik, hvor den berørte tredjelandsstatsborger forlader Schengenområdet, til indberetningen aktiveres i SIS. Dette bør sikre håndhævelse af indrejseforbud ved grænseovergangsstederne ved de ydre grænser og forhindre fornyet indrejse i Schengenområdet.

(27) Personer, over for hvem der er truffet en afgørelse om nægtelse af indrejse og ophold, bør have ret til at påklage denne afgørelse. Klageretten bør være i overensstemmelse med direktiv 2008/115/EF, hvor afgørelsen vedrører tilbagesendelse.

[1] Europa-Parlamentets og Rådets direktiv 2008/115/EF af 16. december 2008 om fælles standarder og procedurer i medlemsstaterne for tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold (EUT L 348 af 24.12.2008, s. 98).

(28) Ved denne forordning bør der fastsættes ufravigelige regler om konsultation og underretning af nationale myndigheder, hvor en tredjelandsstatsborger er indehaver af eller kan erhverve en gyldig opholdstilladelse eller et visum til længerevarende ophold, der er udstedt i én medlemsstat, og en anden medlemsstat agter at indlæse eller allerede har indlæst en indberetning om nægtelse af indrejse og ophold for den pågældende tredjelandsstatsborger. Disse situationer skaber alvorlig usikkerhed for grænsevagter, politi og immigrationsmyndigheder. Derfor er det hensigtsmæssigt at fastsætte bestemmelser om en obligatorisk frist for hurtig konsultation, som fører til et endeligt resultat, for at sikre, at tredjelandsstatsborgere, der har ret til at tage lovligt ophold på medlemsstaternes område, har ret til indrejse på dette område uden vanskeligheder, og at de personer, der ikke er berettiget til indrejse, forhindres heri.

(29) Når en indberetning i SIS slettes efter en konsultation mellem medlemsstaterne, bør den indberettende medlemsstat kunne beholde den pågældende tredjelandsstatsborger på sin nationale indberetningsliste.

(30) Denne forordning bør ikke berøre anvendelsen af Europa-Parlamentets og Rådets direktiv 2004/38/EF[1].

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

(31) Indberetninger bør ikke opbevares længere i SIS, end det er nødvendigt af hensyn til de specifikke formål, der lå til grund for, at de blev indlæst. Inden tre år efter, at den har indlæst en indberetning i SIS, bør den indberettende medlemsstat undersøge behovet for fortsat at opbevare den. Hvis den nationale afgørelse, som indberetningen er baseret på, fastsætter en længere gyldighedsperiode end tre år, bør indberetningen dog undersøges inden for fem år. Beslutningerne om at opbevare indberetninger om personer bør baseres på en samlet individuel vurdering. Medlemsstaterne bør undersøge indberetninger om personer inden for den fastsatte undersøgelsesfrist og bør føre statistik over antallet af indberetninger om personer, i forbindelse med hvilke opbevaringsfristen er blevet forlænget.

(32) Ved indlæsning af en indberetning i SIS og forlængelse af udløbsdatoen for en indberetning i SIS bør den fornødne proportionalitet sikres, herunder ved undersøgelse af, om en konkret sag er egnet, relevant og vigtig nok til at retfærdiggøre, at der indlæses en indberetning i SIS. Når det drejer sig om terrorhandlinger, bør sagen anses for at være egnet, relevant og vigtig nok til at retfærdiggøre en indberetning i SIS. Af hensyn til den offentlige eller nationale sikkerhed bør medlemsstaterne undtagelsesvis kunne undlade at indlæse en indberetning i SIS, når det er sandsynligt, at dette kan hindre officielle eller retlige undersøgelser, efterforskninger eller procedurer.

(33) SIS-oplysningernes integritet er af allerstørste betydning. Derfor bør der fastsættes fornødne sikkerhedsforanstaltninger ved behandling af SIS-oplysninger på centralt og nationalt plan for at sikre oplysningernes "end-to-end"-sikkerhed. De myndigheder, der er involveret i databehandling, bør være underlagt sikkerhedskravene i denne forordning og en ensartet procedure for rapportering af hændelser. Deres medarbejdere bør være korrekt uddannet til formålet og være underrettet om alle lovovertrædelser og strafferetlige sanktioner i forbindelse hermed.

(34) Oplysninger, der er behandlet i SIS, og de tilknyttede supplerende oplysninger, der er udvekslet i henhold til denne forordning, bør ikke overføres eller stilles til rådighed for tredjelande eller internationale organisationer.

(35) For at effektivisere immigrationsmyndighedernes arbejde, når de træffer afgørelser om tredjelandsstatsborgeres ret til indrejse og ophold på medlemsstaternes område og om tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold, er det hensigtsmæssigt ved denne forordning at give disse myndigheder adgang til SIS.

(36) Uden at dette berører de mere specifikke regler i denne forordning om behandling af personoplysninger, bør forordning (EU) 2016/679 finde anvendelse på medlemsstaternes behandling af personoplysninger i medfør af nærværende forordning, medmindre en sådan behandling foretages af nationale kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge terrorhandlinger eller andre alvorlige strafbare handlinger.

(37) Uden at dette berører de mere specifikke regler i denne forordning, bør de nationale love og administrative bestemmelser, der vedtages i henhold til direktiv (EU) 2016/680, finde anvendelse på behandling af personoplysninger, der i medfør af denne forordning foretages af nationale kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge terrorhandlinger eller andre alvorlige strafbare handlinger. Adgang til oplysninger, der indlæses i SIS, og ret til at søge i disse oplysninger for nationale kompetente myndigheder med ansvar for at forebygge, afsløre, efterforske eller retsforfølge terrorhandlinger eller andre alvorlige strafbare handlinger eller for at fuldbyrde strafferetlige sanktioner skal være underlagt alle relevante bestemmelser i denne forordning samt i direktiv (EU) 2016/680 som gennemført i national ret, og navnlig tilsyn ført af de tilsynsmyndigheder, der er omhandlet i direktiv (EU) 2016/680.

(38) Europa-Parlamentets og Rådets forordning (EU) 2018/…[1+] bør finde anvendelse på behandling af personoplysninger, der foretages af Unionens institutioner og organer, når de varetager deres opgaver i medfør af nærværende forordning.

---

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

[+] EUT: Indsæt venligst nummeret i teksten og udfyld EUT-henvisningen i fodnoten for forordningen i PE-CONS 31/18.

(39) Europa-Parlamentets og Rådets forordning (EU) 2016/794[1] bør finde anvendelse på Europols behandling af personoplysninger i medfør af nærværende forordning.

(40) Ved anvendelsen af SIS bør de kompetente myndigheder sikre, at værdigheden og integriteten for den person, hvis oplysninger behandles, respekteres. Behandling af personoplysninger i henhold til denne forordning må ikke medføre forskelsbehandling af personer på grund af køn, race eller etnisk oprindelse, religion eller tro, handicap, alder eller seksuel orientering.

(41) For så vidt angår fortrolighed bør de relevante bestemmelser i vedtægten for tjenestemænd i Den Europæiske Union og ansættelsesvilkårene for de øvrige ansatte Unionen, jf. Rådets forordning (EØF, Euratom, EKSF) nr. 259/68[2] ("personalevedtægten"), finde anvendelse på de tjenestemænd eller øvrige ansatte, der er ansat og arbejder i forbindelse med SIS.

(42) Både medlemsstaterne og eu-LISA bør råde over sikkerhedsplaner for at lette gennemførelsen af sikkerhedsforpligtelser og bør samarbejde indbyrdes for at behandle sikkerhedsspørgsmål ud fra et fælles perspektiv.

---

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

[2] EFT L 56 af 4.3.1968, s. 1.

(43) De nationale uafhængige tilsynsmyndigheder, der er omhandlet i forordning (EU) 2016/679 og direktiv (EU) 2016/680 ("tilsynsmyndighederne"), bør overvåge lovligheden af medlemsstaternes behandling af personoplysninger i medfør af nærværende forordning, herunder udveksling af supplerende oplysninger. Tilsynsmyndighederne bør tildeles de fornødne ressourcer til at udføre denne opgave. Der bør fastsættes bestemmelser om de registreredes ret til adgang til, berigtigelse og sletning af deres personoplysninger, som er opbevaret i SIS, og deres adgang til eventuelle efterfølgende retsmidler ved nationale domstole samt om gensidig anerkendelse af domme. Det er også hensigtsmæssigt at kræve årlige statistikker fra medlemsstaterne.

(44) Tilsynsmyndighederne bør sikre, at der mindst hvert fjerde år foretages en audit af databehandlingsaktiviteterne i deres medlemsstats nationale systemer i overensstemmelse med internationale standarder for audit. Denne audit bør enten foretages af tilsynsmyndighederne, eller tilsynsmyndighederne bør bestille auditten direkte hos en uafhængig auditor med ekspertise inden for databeskyttelse. Den uafhængige auditor bør forblive under de pågældende tilsynsmyndigheders kontrol og ansvar, og disse bør derfor selv instruere auditten og fastlægge et klart defineret formål og anvendelsesområde og en klart defineret metode for auditten samt fremlægge retningslinjer og foretage tilsyn med hensyn til auditten og dens endelige resultater.

(45) Den Europæiske Tilsynsførende for Databeskyttelse bør overvåge Unionens institutioners og organers aktiviteter i forbindelse med behandling af personoplysninger i medfør af denne forordning. Den Europæiske Tilsynsførende for Databeskyttelse og tilsynsmyndighederne bør samarbejde om tilsynet med SIS.

(46) Den Europæiske Tilsynsførende for Databeskyttelse bør have tilstrækkelige ressourcer til at kunne udføre de opgaver, som den pålægges ved denne forordning, herunder bistand fra personer med ekspertise inden for biometriske data.

(47) I forordning (EU) 2016/794 fastsættes det, at Europol skal støtte og styrke de kompetente nationale myndigheders indsats og deres samarbejde om bekæmpelse af terrorisme og grov kriminalitet og udarbejde analyser og trusselsvurderinger. For at gøre det lettere for Europol at varetage sine opgaver, navnlig inden for rammerne af Det Europæiske Center for Migrantsmugling, er det hensigtsmæssigt at give Europol adgang til indberetningskategorier fastsat i nærværende forordning.

(48) For at lukke hullerne med hensyn til udveksling af oplysninger om terrorisme, navnlig om fremmedkrigere i tilfælde, hvor overvågning af deres bevægelser er afgørende, opfordres medlemsstaterne til at dele oplysninger om terrorismerelateret aktivitet med Europol. Denne deling af oplysninger bør ske ved at udveksle supplerende oplysninger med Europol om de berørte indberetninger. Til dette formål bør Europol oprette en forbindelse til kommunikationsinfrastrukturen.

(49) Det er desuden nødvendigt at fastsætte klare regler for Europol om behandling og download af SIS-oplysninger, så det kan gøre omfattende brug af SIS, forudsat at databeskyttelsesstandarderne i denne forordning og forordning (EU) 2016/794 overholdes. Hvis Europols søgninger i SIS viser, at der findes en indberetning indlæst af en medlemsstat, kan Europol ikke foretage de påkrævede handlinger. Det bør derfor underrette den pågældende medlemsstat via udveksling af supplerende oplysninger med det respektive SIRENE-kontor, således at nævnte medlemsstat kan følge op på sagen.

(50) I Europa-Parlamentets og Rådets forordning (EU) 2016/1624[1] er det med henblik på nævnte forordning fastsat, at værtsmedlemsstaten skal give tilladelse til, at medlemmerne af de hold, der er omhandlet i artikel 2, nr. 8), i nævnte forordning, og som Det Europæiske Agentur for Grænse- og Kystbevogtning har indsat, kan foretage de søgninger i EU-databaser, der er nødvendige for at opfylde de operative mål, der er fastlagt i den operative plan om ind- og udrejsekontrol, grænseovervågning og tilbagesendelse. Andre relevante EU-agenturer, navnlig Det Europæiske Asylstøttekontor og Europol, kan også indsætte eksperter, der ikke er ansat hos disse EU-agenturer, som en del af deres migrationsstyringsstøttehold. Hensigten med udsendelsen af de hold, der er omhandlet i artikel 2, nr. 8) og 9), i nævnte forordning, er at give de medlemsstater, der anmoder om det, teknisk og operativ støtte, navnlig de medlemsstater, der står over for uforholdsmæssigt store migrationsudfordringer. For at de hold, der er omhandlet i artikel 2, nr. 8) og 9), i nævnte forordning, kan varetage deres opgaver, har de brug for adgang til SIS via en teknisk grænseflade hos Det Europæiske Agentur for Grænse- og Kystbevogtning med forbindelse til det centrale SIS. I de tilfælde, hvor søgninger i SIS foretaget af de hold, der er omhandlet i artikel 2, nr. 8) og 9), i forordning (EU) 2016/1624, eller holdene af medarbejdere registrerer en indberetning indlæst af en medlemsstat, må holdmedlemmet eller medarbejderen ikke foretage de påkrævede handlinger, medmindre værtsmedlemsstaten har givet tilladelse dertil. Derfor bør værtsmedlemsstaten underrettes, så den kan følge op på sagen. Værtsmedlemsstaten bør underrette den indberettende medlemsstat om hittet via udveksling af supplerende oplysninger.

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

(51) Visse aspekter af SIS kan ikke dækkes udtømmende af denne forordning på grund af deres tekniske, stærkt detaljerede og hyppigt ændrende karakter. Disse aspekter omfatter f.eks. tekniske regler om indlæsning af oplysninger, om ajourføring, sletning og søgning efter oplysninger og om datakvalitet og regler vedrørende biometriske data, regler om indberetningers kompatibilitet og prioritetsrækkefølge, sammenkobling af indberetninger og udveksling af supplerende oplysninger. Gennemførelsesbeføjelser i forbindelse med disse aspekter bør derfor tillægges Kommissionen. De tekniske regler for søgning i indberetninger bør tage hensyn til, at de nationale applikationer skal fungere problemfrit.

(52) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011[1]. Proceduren for vedtagelse af gennemførelsesretsakter i medfør af nærværende forordning og forordning (EU) 2018/...[+] bør være den samme.

(53) For at sikre gennemsigtighed bør eu-LISA to år efter idriftsættelsen af SIS i henhold til denne forordning udarbejde en rapport om det centrale SIS-systems og kommunikationsinfrastrukturens tekniske funktion, herunder om sikkerheden i forbindelse hermed, og om den bilaterale og multilaterale udveksling af supplerende oplysninger. Kommissionen bør hvert fjerde år udsende en samlet evaluering.

---

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

[+] EUT: Indsæt venligst nummeret på forordningen i PE-CONS 36/18

(54) For at sikre at SIS kan fungere gnidningsløst, bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF, for så vidt angår fastlæggelsen af under hvilke omstændigheder fotografier og ansigtsbilleder kan anvendes til identifikation af personer bortset fra ved almindelige grænseovergangssteder. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning[1]. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(55) Målene for denne forordning, nemlig oprettelse og regulering af et EU-informationssystem og udveksling af tilknyttede supplerende oplysninger, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af deres karakter bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union (TEU). I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre end, hvad der er nødvendigt for at nå disse mål.

[1] EUT L 123 af 12.5. 2016, s. 1.

(56) Denne forordning overholder de grundlæggende rettigheder og de principper, som navnlig anerkendes i Den Europæiske Unions charter om grundlæggende rettigheder. Denne forordning overholder navnlig fuldt ud beskyttelsen af personoplysninger i overensstemmelse med artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder og søger samtidig at garantere et sikkert miljø for alle personer, der opholder sig på Unionens område, og beskyttelse af irregulære migranter mod udnyttelse og menneskehandel. I sager vedrørende børn bør barnets tarv komme i første række.

(57) De anslåede omkostninger ved den opgradering af de nationale systemer og den gennemførelse af de nye funktioner, der er forudset i denne forordning, er lavere end det resterende beløb på budgetposten for intelligente grænser i Europa-Parlamentet og Rådets forordning (EU) nr. 515/2014[1]. Derfor bør de midler, der er afsat til udvikling af IT-systemer, der understøtter forvaltningen af migrationsstrømme på tværs af de ydre grænser, jf. forordning (EU) nr. 515/2014, allokeres til medlemsstaterne og eu-LISA. De finansielle omkostninger ved opgradering af SIS og gennemførelse af nærværende forordning bør overvåges. Hvis de anslåede omkostninger er højere, bør der stilles EU-midler til rådighed til at støtte medlemsstaterne i overensstemmelse med den relevante flerårige finansielle ramme.

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

(58) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til TEU og TEUF, deltager Danmark ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Danmark. Inden seks måneder efter, at Rådet har truffet foranstaltning om denne forordning til udbygning af Schengenreglerne, træffer Danmark afgørelse om, hvorvidt det vil gennemføre denne forordning i sin nationale lovgivning, jf. artikel 4 i protokollen.

(59) Denne forordning udgør en udvikling af de bestemmelser i Schengenreglerne, som Det Forenede Kongerige ikke deltager i, jf. Rådets afgørelse 2000/365/EF[1]; Det Forenede Kongerige deltager derfor ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Det Forenede Kongerige.

(60) Denne forordning udgør en udvikling af de bestemmelser i Schengenreglerne, som Irland ikke deltager i, jf. Rådets afgørelse 2002/192/EF[2]; Irland deltager derfor ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Irland.

---

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

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

(61) For så vidt angår Island og Norge udgør denne forordning en udvikling af de bestemmelser i Schengenreglerne, jf. aftalen indgået mellem Rådet for Den Europæiske Union og Republikken Island og Kongeriget Norge om disse to staters associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne[1], der henhører under det område, der er nævnt i artikel 1, litra G), i Rådets afgørelse 1999/437/EF[2].

(62) For så vidt angår Schweiz udgør denne forordning en udvikling af de bestemmelser i Schengenreglerne, jf. aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne[3], der henhører under det område, der er nævnt i artikel 1, litra G), i afgørelse 1999/437/EF sammenholdt med artikel 3 i Rådets afgørelse 2008/146/EF[4].

---

1 EFT L 176 af 10.7.1999, s. 36.

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

3 EUT L 53 af 27.2. 2008, s. 52.

4 Rådets afgørelse 2008/146/EF af 28. januar 2008 om indgåelse, på Det Europæiske Fællesskabs vegne, af aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne (EUT L 53 af 27.2.2008, s. 1).

(63) For så vidt angår Liechtenstein udgør denne forordning en udvikling af de bestemmelser i Schengenreglerne, jf. protokollen mellem Den Europæiske Union, Det Europæiske Fællesskab, Det Schweiziske Forbund og Fyrstendømmet Liechtenstein om Fyrstendømmet Liechtensteins tiltrædelse af aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengenreglerne[1], der henhører under det område, der er nævnt i artikel 1, litra G), i afgørelse 1999/437/EF sammenholdt med artikel 3 i Rådets afgørelse 2011/350/EU[2].

(64) For så vidt angår Bulgarien og Rumænien udgør denne forordning en retsakt, der bygger på, eller som på anden måde har tilknytning til, Schengenreglerne, jf. artikel 4, stk. 2, i tiltrædelsesakten af 2005, og bør sammenholdes med Rådets afgørelse 2010/365/EU[3] og (EU) 2018/934[4].

---

1 EUT L 160 af 18.6. 2011, s. 21.

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

3 Rådets afgørelse 2010/365/EU af 29. juni 2010 om anvendelse af Schengenreglernes bestemmelser om Schengeninformationssystemet i Republikken Bulgarien og Rumænien (EUT L 166 af 1.7.2010, s. 17).

4 Rådets afgørelse (EU) 2018/934 af 25. juni 2018 om anvendelsen af de resterende bestemmelser i Schengenreglerne om Schengeninformationssystemet i Republikken Bulgarien og Rumænien (EUT L 165 af 2.7.2018, s. 37).

(65) For så vidt angår Kroatien udgør denne forordning en retsakt, der bygger på, eller som på anden måde har tilknytning til, Schengenreglerne, jf. artikel 4, stk. 2, i tiltrædelsesakten af 2011, og bør sammenholdes med Rådets afgørelse (EU) 2017/733[1].

(66) For så vidt angår Cypern udgør denne forordning en retsakt, der bygger på, eller som på anden måde har tilknytning til, Schengenreglerne, jf. artikel 3, stk. 2, i tiltrædelsesakten af 2003.

(67) Ved denne forordning indføres en række forbedringer af SIS, som vil øge effektiviteten, styrke databeskyttelsen og udvide adgangsrettighederne. Visse af disse forbedringer kræver ikke en kompleks teknisk udvikling, mens andre faktisk kræver tekniske ændringer af forskellig størrelsesorden. For at gøre det muligt at stille forbedringer af systemet til rådighed for slutbrugerne så snart som muligt foretages der med denne forordning ændringer af forordning (EF) nr. 1987/2006 i flere faser. En række forbedringer af systemet bør finde anvendelse omgående efter nærværende forordnings ikrafttræden, mens andre bør finde anvendelse enten et eller to år efter dens ikrafttræden. Nærværende forordning bør anvendes i alle enkeltheder senest tre år efter dens ikrafttræden. For at undgå forsinkelser i anvendelsen heraf bør den trinvise gennemførelse af nærværende forordning overvåges nøje.

---

[1] Rådets afgørelse (EU) 2017/733 af 25. april 2017 om anvendelsen af bestemmelserne i Schengenreglerne for så vidt angår Schengeninformationssystemet i Republikken Kroatien (EUT L 108 af 26.4.2017, s. 31).

(68) Rådets forordning (EF) nr. 1987/2006 bør ophæves med virkning fra den dato, hvor nærværende forordning finder anvendelse i sin helhed.

(69) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 28, stk. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001[1], og afgav en udtalelse den 3. maj 2017 —

VEDTAGET DENNE FORORDNING:

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

Kapitel I
Generelle bestemmelser

Artikel 1

SIS' generelle formål

SIS har til formål at sikre et højt sikkerhedsniveau inden for Unionens område med frihed, sikkerhed og retfærdighed ved hjælp af oplysningerne meddelt via dette system, herunder at opretholde den offentlige sikkerhed og den offentlige orden samt beskytte sikkerheden på medlemsstaternes område og at sikre anvendelsen af bestemmelserne i tredje del, afsnit V, kapitel 2, i TEUF vedrørende persontrafik på deres område.

Artikel 2

Genstand

1. I denne forordning fastsættes betingelserne og procedurerne for indlæsning og behandling af indberetninger i SIS vedrørende tredjelandsstatsborgere og for udvekslingen af supplerende og uddybende oplysninger med henblik på nægtelse af indrejse og ophold på medlemsstaternes område.

2. I denne forordning fastsættes også bestemmelser vedrørende SIS' tekniske arkitektur, det ansvar, der påhviler medlemsstaterne og Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA), databehandling, de berørte personers rettigheder og erstatningsansvar.

Artikel 3

Definitioner

I denne forordning forstås ved:

1) "indberetning": et sæt oplysninger, der er indlæst i SIS, således at de kompetente myndigheder kan identificere en person med henblik på at foretage en konkret handling

2) "supplerende oplysninger": oplysninger, som ikke indgår som en del af de indberetningsoplysninger, der er lagret i SIS, men som har tilknytning til indberetninger i SIS, og som skal udveksles via SIRENE-kontorerne:

   a) for at gøre det muligt for medlemsstaterne at konsultere eller underrette hinanden i forbindelse med indlæsning af en indberetning

   b) når en søgning har givet et hit, således at den rette handling kan foretages

   c) når den påkrævede handling ikke kan foretages

d) i spørgsmål vedrørende kvaliteten af SIS-oplysningerne

e) i spørgsmål vedrørende indberetningers kompatibilitet og prioritet

f) i spørgsmål vedrørende adgangsrettigheder

3) "uddybende oplysninger": de oplysninger, der er lagret i SIS og har tilknytning til indberetninger i SIS, og som omgående skal være til rådighed for de kompetente myndigheder, hvor en person, om hvem der er indlæst oplysninger i SIS, lokaliseres som følge af en søgning i SIS

4) "tredjelandsstatsborger": enhver person, der ikke er unionsborger i henhold til artikel 20, stk. 1, i TEUF, med undtagelse af personer, som er berettiget til fri bevægelighed svarerende til unionsborgere i henhold til aftaler mellem Unionen eller Unionen og dens medlemsstater på den ene side og et tredjeland på den anden side

5) "personoplysninger": personoplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679

6) "behandling af personoplysninger": enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, såsom indsamling, registrering, logning, organisering, systematisering, lagring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved overførsel, formidling eller enhver anden form for tilgængeliggørelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

7) "match": forekomsten af følgende trin:

a) en slutbruger har foretaget en søgning i SIS

b) denne søgning har vist, at en anden medlemsstat har indlæst en indberetning i SIS, og

c) oplysninger vedrørende indberetningen i SIS svarer til søgeoplysningerne

8) "hit": ethvert match, som opfylder følgende kriterier:

a) det er blevet bekræftet af:

i) slutbrugeren, eller

ii) den kompetente myndighed i overensstemmelse med nationale procedurer, hvor det pågældende match var baseret på en sammenligning af biometriske data,

og

b) der kræves yderligere handlinger

9) "indberettende medlemsstat": den medlemsstat, der indlæste indberetningen i SIS

10) "udstedende medlemsstat": den medlemsstat, der overvejer at udstede eller forlænge eller har udstedt eller forlænget en opholdstilladelse eller et visum til længerevarende ophold og er involveret i konsultationsproceduren med en anden medlemsstat

11) "fuldbyrdende medlemsstat": den medlemsstat, der foretager eller har foretaget de påkrævede handlinger på baggrund af et hit

12) "slutbruger": en medarbejder hos en kompetent myndighed, der er bemyndiget til at søge direkte i CS-SIS, N.SIS eller en teknisk kopi heraf

13) "biometriske data": personoplysninger, der som følge af en specifik teknisk behandling vedrørende en fysisk persons fysiske eller fysiologiske kendetegn muliggør eller bekræfter en entydig identifikation af vedkommende, nemlig fotografier, ansigtsbilleder og fingeraftryksoplysninger

14) "fingeraftryksoplysninger": oplysninger om fingeraftryk og håndfladeaftryk, som på grund af deres unikke karakter og referencepunkterne i dem gør det muligt at foretage præcise og endegyldige sammenligninger vedrørende en persons identitet

15) "ansigtsbillede": digitale billeder af ansigtet med tilstrækkelig opløsning og kvalitet til, at de kan anvendes i forbindelse med automatisk biometrisk sammenligning

16) "tilbagesendelse": tilbagesendelse som defineret i artikel 3, nr. 3), i direktiv 2008/115/EF

17) "indrejseforbud": et indrejseforbud som defineret i artikel 3, nr. 6), i direktiv 2008/115/EF

18) "terrorhandlinger": lovovertrædelser i henhold til national ret, der er omhandlet i artikel 3-14 i Europa-Parlamentets og Rådets direktiv (EU) 2017/541[1] eller svarer til en af disse lovovertrædelser i de medlemsstater, der ikke er bundet af nævnte direktiv

19) "opholdstilladelse": en opholdstilladelse som defineret i artikel 2, nr. 16), i Europa-Parlamentets og Rådets forordning (EU) 2016/399[2]

20) "visum til længerevarende ophold": et visum til længerevarende ophold som omhandlet i artikel 18, stk. 1, i konventionen om gennemførelse af Schengenaftalen

21) "trussel mod den offentlige sundhed": en trussel mod den offentlige sundhed som defineret i artikel 2, nr. 21), i forordning (EU) 2016/399.

Artikel 4

SIS' tekniske arkitektur og driftsmåder

1. SIS består af:

a) et centralt system (det centrale SIS) bestående af:

i) en teknisk støttefunktion ("CS-SIS"), som indeholder en database, "SIS-databasen", herunder en CS-SIS-backup

---

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

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

ii) en ensartet national grænseflade ("NI-SIS")

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

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

Et N.SIS som omhandlet i litra b) kan indeholde en datafil (en "national kopi"), som indeholder en fuldstændig eller delvis kopi af SIS-databasen. To eller flere medlemsstater kan i et af deres N.SIS'er oprette en delt kopi, der kan benyttes i fællesskab af disse medlemsstater. En sådan delt kopi betragtes som hver af disse medlemsstaters nationale kopi.

En delt N.SIS-backup som omhandlet i litra b) kan benyttes i fællesskab af to eller flere medlemsstater. I sådanne tilfælde betragtes den delte N.SIS-backup som hver af disse medlemsstaters N.SIS-backup. N.SIS og backuppen heraf kan anvendes samtidigt for at sikre, at systemet altid er tilgængeligt for slutbrugerne.

Medlemsstater, der har til hensigt at oprette en delt kopi eller delt N.SIS-backup, som skal benyttes i fællesskab, fastlægger deres respektive ansvarsområder skriftligt. De meddeler deres ordning til Kommissionen.

Kommunikationsinfrastrukturen støtter og bidrager til at sikre SIS' uafbrudte tilgængelighed. Den omfatter redundante og adskilte stier for forbindelserne mellem CS-SIS og CS-SIS-backuppen og omfatter også redundante og adskilte stier for forbindelser mellem hvert nationale SIS-netadgangspunkt og CS-SIS og CS-SIS-backuppen.

2. Medlemsstaterne indlæser, ajourfører, sletter og søger SIS-oplysninger via deres eget N.SIS. De medlemsstater, der anvender en delvis eller fuldstændig national kopi eller en delvis eller fuldstændig delt kopi, stiller denne kopi til rådighed med henblik på elektroniske søgninger på hver af disse medlemsstaters område. Den delvise nationale eller delte kopi indeholder som minimum de oplysninger, der er omhandlet i artikel 20, stk. 2, litra a)-v). Det må ikke være muligt at søge i andre medlemsstaters N.SIS-datafiler, undtagen i tilfælde af delte kopier.

3. CS-SIS udfører tekniske tilsyns- og forvaltningsfunktioner og har en CS-SIS-backup, der kan sikre alle funktionaliteterne i CS-SIS, hvis dette system skulle svigte. CS-SIS og CS-SIS-backuppen placeres i eu-LISA's to tekniske anlæg.

4. eu-LISA gennemfører tekniske løsninger for at styrke den uafbrudte tilgængelighed af SIS enten gennem samtidig drift af CS-SIS og CS-SIS-backuppen, forudsat at CS-SIS-backuppen forbliver i stand til at sikre driften af SIS, hvis CS-SIS skulle svigte, eller gennem duplikering af systemet eller dets dele. Uanset de proceduremæssige krav i artikel 10 i forordning (EU) 2018/…[+] foretager eu-LISA senest den ... [et år efter denne forordnings ikrafttræden] en undersøgelse om mulighederne for tekniske løsninger, indeholdende en uafhængig konsekvensvurdering og cost-benefit-analyse.

5. Om nødvendigt kan eu-LISA i exceptionelle tilfælde midlertidigt udvikle en yderligere kopi af SIS-databasen.

6. CS-SIS stiller de tjenester til rådighed, som er nødvendige for indlæsningen og behandlingen af SIS-oplysninger, herunder søgning i SIS-databasen. For de medlemsstater, der anvender en national eller en delt kopi, skal CS-SIS:

   a) sørge for onlineopdateringer til de nationale kopier

   b) sikre synkroniseringen og sammenhængen mellem de nationale kopier og SIS-databasen, og

   c) sørge for operationen med henblik på initialisering og genopretning af de nationale kopier.

7. CS-SIS sørger for uafbrudt tilgængelighed.

[+] EUT: Indsæt venligst løbenummeret for forordningen i PE-CONS 29/18.

Artikel 5

Udgifter

1. Udgifterne til drift, vedligeholdelse og videreudvikling af det centrale SIS og kommunikationsinfrastrukturen afholdes over Unionens almindelige budget. Disse udgifter omfatter arbejde med CS-SIS for at sikre, at de tjenester, der er omhandlet i artikel 4, stk. 6, stilles til rådighed.

2. Der afsættes midler fra finansieringsrammen på 791 mio. EUR, jf. artikel 5, stk. 5, litra b), i forordning (EU) nr. 515/2014 til at dække omkostningerne ved gennemførelsen af nærværende forordning.

3. Fra finansieringsrammen omhandlet i stk. 2 og med forbehold af yderligere midler til dette formål fra andre kilder i Unionens almindelige budget afsættes et beløb på 31 098 000 EUR til eu-LISA. En sådan finansiering gennemføres ved indirekte forvaltning og bidrager til at gennemføre den tekniske udvikling, der kræves i henhold til denne forordning vedrørende det centrale SIS og kommunikationsinfrastrukturen samt dermed forbundne uddannelsesaktiviteter.

4. Fra finansieringsrammen omhandlet i stk. 2 modtager de medlemsstater, der deltager i forordning (EU) nr. 515/2014, en ekstra samlet bevilling på 36 810 000 EUR, der fordeles i lige dele som et fast beløb til deres basistildeling. Denne finansiering gennemføres ved delt forvaltning og anvendes fuldt ud til hurtig og effektiv opgradering af det berørte nationale system i overensstemmelse med kravene i nærværende forordning.

5. Udgifterne til oprettelse, drift, vedligeholdelse og videreudvikling af hvert N.SIS dækkes af den pågældende medlemsstat.

Kapitel II

Medlemsstaternes ansvar

Artikel 6

Nationale systemer

Hver medlemsstat er ansvarlig for at oprette, drive, vedligeholde og videreudvikle sit N.SIS og for at forbinde det med NI-SIS.

Hver medlemsstat er ansvarlig for at sikre uafbrudt tilgængelighed af SIS-oplysninger for slutbrugerne.

Hver medlemsstat foretager sine indberetninger via sit N.SIS.

Artikel 7

N.SIS- og SIRENE-kontoret

1. Hver medlemsstat udpeger en myndighed (N.SIS-kontoret), der har det overordnede ansvar for dets N.SIS.

   Denne myndighed er ansvarlig for, at N.SIS fungerer sikkert og gnidningsløst, sikrer, at de kompetente myndigheder har adgang til SIS, og træffer de nødvendige foranstaltninger til at sikre overholdelse af denne forordning. Den har ansvaret for at sikre, at alle funktionaliteter i SIS på hensigtsmæssig vis stilles til rådighed for slutbrugerne.

2. Hver medlemsstat udpeger en national myndighed, der skal være operationel døgnet rundt alle ugens dage, og som sikrer udvekslingen og tilgængeligheden af alle supplerende oplysninger (SIRENE-kontoret), i overensstemmelse med SIRENE-håndbogen. Hvert SIRENE-kontor skal være et fælles kontaktpunkt for dets medlemsstat med henblik på at udveksle supplerende oplysninger i forbindelse med indberetninger og gøre det lettere at foretage de påkrævede handlinger, når der er indlæst indberetninger om personer i SIS, og disse personer lokaliseres efter et hit.

   Hvert SIRENE-kontor skal i overensstemmelse med national ret have let direkte eller indirekte adgang til alle relevante nationale oplysninger, herunder nationale databaser og alle oplysninger vedrørende dets medlemsstats egne indberetninger, og til ekspertrådgivning, for at kunne reagere på anmodninger om supplerende oplysninger hurtigt og inden for fristerne i artikel 8.

SIRENE-kontorerne samordner kontrollen af kvaliteten af de oplysninger, der indlæses i SIS. Med henblik herpå har de adgang til de oplysninger, der behandles i SIS.

3. Medlemsstaterne giver eu-LISA de nærmere oplysninger om deres N.SIS -kontor og deres SIRENE-kontor. eu-LISA offentliggør listen over N.SIS-kontorerne og SIRENE-kontorerne sammen med den liste, der er omhandlet i artikel 41, stk. 8.

Artikel 8

Udveksling af supplerende oplysninger

1. Supplerende oplysninger udveksles i overensstemmelse med bestemmelserne i SIRENE-håndbogen og ved hjælp af kommunikationsinfrastrukturen. Medlemsstaterne sikrer de nødvendige tekniske og menneskelige ressourcer til at sikre konstant tilgængelighed og rettidig og effektiv udveksling af supplerende oplysninger. Hvis kommunikationsinfrastrukturen ikke er tilgængelig, anvender medlemsstaterne andre tilstrækkeligt sikrede tekniske midler til at udveksle supplerende oplysninger. En liste over tilstrækkeligt sikrede tekniske midler fastsættes i SIRENE-håndbogen.

2. Supplerende oplysninger må kun anvendes til det formål, hvortil de blev videregivet, jf. artikel 49, medmindre der er indhentet forudgående samtykke til anden anvendelse fra den indberettende medlemsstat.

3. SIRENE-kontorerne varetager deres opgaver hurtigt og effektivt, navnlig ved give svar på en anmodning om supplerende oplysninger hurtigst muligt og senest 12 timer efter modtagelsen af anmodningen.

Anmodninger om supplerende oplysninger med den højeste prioritet forsynes med påskriften "URGENT" i SIRENE-formularerne ledsaget af begrundelsen for sagens hastende karakter.

4. Kommissionen vedtager gennemførelsesretsakter med henblik på at fastsætte detaljerede regler om SIRENE-kontorernes opgaver i medfør af denne forordning og udveksling af supplerende oplysninger i form af en håndbog med titlen "SIRENE-håndbogen". Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

Artikel 9

Teknisk og funktionel overensstemmelse

1. Hver medlemsstat overholder ved oprettelsen af sit N.SIS de fælles standarder, protokoller og tekniske procedurer, der er fastsat for at sikre, at dets N.SIS er kompatibelt med det centrale SIS med henblik på en hurtig og effektiv overførsel af oplysninger.

2. Hvis en medlemsstat anvender en national kopi, skal den ved hjælp af de tjenester, som CS-SIS stiller til rådighed, og via de automatiske opdateringer, der er omhandlet i artikel 4, stk. 6, sikre, at de oplysninger, der er lagret i den nationale kopi, er identiske og i overensstemmelse med SIS-databasen, og at en søgning i dens nationale kopi giver et søgeresultat, der svarer til resultatet af en søgning i SIS-databasen.

3. Slutbrugerne modtager de oplysninger, der er nødvendige for, at de kan varetage deres opgaver, navnlig, og for så vidt det er nødvendigt, alle de tilgængelige oplysninger, der gør det muligt at identificere de registrerede og at foretage den påkrævede handling.

4. Medlemsstaterne og eu-LISA foretager regelmæssigt tests for at verificere den tekniske overensstemmelse af de nationale kopier, jf. stk. 2. Der skal tages hensyn til disse tests som led i den mekanisme, der blev oprettet ved Rådets forordning (EU) nr. 1053/2013[1].

5. Kommissionen vedtager gennemførelsesretsakter med henblik på fastsættelse og udarbejdelse af de i denne artikels stk. 1 omhandlede fælles standarder, protokoller og tekniske procedurer. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

[1] Rådets forordning (EU) nr. 1053/2013 af 7. oktober 2013 om indførelse af en evaluerings- og overvågningsmekanisme til kontrol af anvendelsen af Schengenreglerne og om ophævelse af Eksekutivkomitéens afgørelse af 16. september 1998 om nedsættelse af et stående udvalg for evaluering og anvendelse af Schengenreglerne (EUT L 295 af 6.11.2013, s. 27).

Artikel 10

Sikkerhed – medlemsstaterne

1. Hver medlemsstat vedtager i relation til sit N.SIS de nødvendige foranstaltninger, herunder en sikkerhedsplan, en driftskontinuitetsplan og en katastrofeberedskabsplan, med henblik på:

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

   b) at forhindre, at uautoriserede personer får adgang til de anlæg, der benyttes til behandling af personoplysninger (kontrol med fysisk adgang til anlæggene)

   c) at forhindre uautoriseret læsning, kopiering, ændring eller sletning af datamedier (kontrol med datamedier)

   d) at forhindre uautoriseret indlæsning af oplysninger samt uautoriseret læsning, ændring eller sletning af lagrede personoplysninger (kontrol med lagring)

   e) at forhindre, at de automatiserede databehandlingssystemer kan benyttes af uautoriserede personer ved hjælp af datakommunikationsudstyr (brugerkontrol)

   f) at forhindre uautoriseret behandling af oplysninger i SIS samt uautoriseret ændring eller sletning af oplysninger, der er behandlet i SIS (kontrol med dataindlæsning)

g) at sikre, at personer, der har tilladelse til at anvende et automatiseret databehandlingssystem, kun har adgang til de oplysninger, der er omfattet af deres adgangstilladelse, ved hjælp af individuelle og entydige brugeridentifikatorer og udelukkende fortrolige adgangstilstande (kontrol med adgang til oplysninger)

h) at sikre, at alle myndigheder med adgangsret til SIS eller til databehandlingsanlæggene opretter profiler, der beskriver funktioner og ansvarsområder for de personer, som har tilladelse til at få adgang til, indlæse, ajourføre, slette og søge i oplysningerne, og straks stiller disse profiler til rådighed for de i artikel 55, stk. 1, omhandlede tilsynsmyndigheder på deres anmodning (personaleprofiler)

i) at sikre, at det er muligt at undersøge og fastslå, til hvilke myndigheder der kan videregives personoplysninger via datakommunikationsudstyr (kontrol med videregivelse)

j) at sikre, at det er muligt efterfølgende at undersøge og fastslå, hvilke personoplysninger der er indlæst i de automatiserede databehandlingssystemer, hvornår, af hvem og til hvilket formål (kontrol med indlæsning)

k) at forhindre uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger i forbindelse med videregivelse af personoplysninger eller under transport af datamedier, navnlig ved hjælp af hensigtsmæssige krypteringsteknikker (transportkontrol)

l) at kontrollere effektiviteten af de sikkerhedsforanstaltninger, der er omhandlet i dette stykke, og træffe de nødvendige organisatoriske foranstaltninger vedrørende intern kontrol for at sikre overholdelsen af denne forordning (egenkontrol)

m) at sikre, at installerede systemer i tilfælde af afbrydelse kan genetableres til normal drift (genopretning), og

n) at sikre, at SIS fungerer korrekt, at fejl rapporteres (pålidelighed), og at personoplysninger lagret i SIS ikke kan ødelægges ved hjælp af systemsvigt (integritet).

2. Medlemsstaterne træffer foranstaltninger svarende til dem, der er omhandlet i stk. 1, for så vidt angår sikkerhed i forbindelse med behandling og udveksling af supplerende oplysninger, herunder sikring af SIRENE-kontorernes lokaler.

3. Medlemsstaterne træffer foranstaltninger svarende til dem, der er omhandlet i denne artikels stk. 1, for så vidt angår sikkerhed i forbindelse med de i artikel 34 omhandlede myndigheders behandling af SIS-oplysninger.

4. De i stk. 1, 2 og 3 beskrevne foranstaltninger kan være led i en generisk sikkerhedsstrategi og -plan på nationalt plan, som omfatter adskillige IT-systemer. I så fald skal de krav, der er fastsat i denne artikel, og deres anvendelse på SIS klart kunne identificeres i og sikres med den pågældende plan.

Artikel 11

Fortrolighed – medlemsstaterne

1. Hver medlemsstat anvender i overensstemmelse med national ret sine egne regler for tavshedspligt eller tilsvarende fortrolighedskrav i forbindelse med alle personer og organer, der skal arbejde med SIS-oplysninger og supplerende oplysninger. Denne pligt fortsætter med at bestå, efter at de pågældende personer er fratrådt deres stilling, eller det pågældende organs virksomhed er ophørt.

2. Hvis en medlemsstat samarbejder med eksterne kontrahenter i forbindelse med SIS-relaterede opgaver, skal den nøje overvåge kontrahentens aktiviteter for at sikre overholdelsen af alle bestemmelser i denne forordning, navnlig med hensyn til sikkerhed, fortrolighed og databeskyttelse.

3. Den operationelle forvaltning af N.SIS eller af tekniske kopier må ikke overdrages til private virksomheder eller private organisationer.

Artikel 12

Opbevaring af logfiler på nationalt plan

1. Medlemsstaterne påser, at hver adgang til og alle udvekslinger af personoplysninger inden for CS-SIS registreres i N.SIS med henblik på at kontrollere, hvorvidt søgningen var lovlig, overvåge databehandlingens lovlighed, udøve egenkontrol, sikre N.SIS' korrekte funktion samt for dataintegritet og datasikkerhed. Dette krav gælder ikke for de automatiske processer, der er omhandlet i artikel 4, stk. 6, litra a), b) og c).

2. Logfilerne skal navnlig vise indberetningens hidtidige forløb, dato og tidspunkt for databehandlingen, de oplysninger, der er anvendt til en søgning, en henvisning til de oplysninger, der er behandlet, samt de individuelle og entydige brugeridentifikatorer for både den kompetente myndighed og den person, der behandler oplysningerne.

3. Hvis en søgning foretages med fingeraftryksoplysninger eller ansigtsbilleder, jf. artikel 33, skal logfilerne som en undtagelse fra nærværende artikels stk. 2 vise den type oplysninger, der er anvendt til søgningen, frem for de faktiske oplysninger.

4. Logfilerne må kun anvendes til det i stk. 1 omhandlede formål og slettes tre år efter deres oprettelse. De logfiler, der indeholder indberetningernes hidtidige forløb, slettes tre år efter, at indberetningerne er slettet.

5. Logfilerne kan opbevares længere end den periode, der er omhandlet i stk. 4, hvis der er brug for dem i forbindelse med kontrolprocedurer, som allerede er indledt.

6. De nationale kompetente myndigheder, der er ansvarlige for at kontrollere, hvorvidt søgninger er lovlige, overvåge databehandlingens lovlighed, udøve egenkontrol og sikre N.SIS' korrekte funktion og dataintegritet og -sikkerhed, skal inden for rammerne af deres beføjelser og efter at have anmodet herom have adgang til logfilerne med henblik på at kunne udføre deres opgaver.

Artikel 13

Egenkontrol

Medlemsstaterne sikrer, at enhver myndighed med adgangsret til SIS-oplysninger træffer de foranstaltninger, der er nødvendige for at sikre overholdelsen af denne forordning, og i nødvendigt omfang samarbejder med tilsynsmyndigheden.

Artikel 14

Uddannelse af personale

1. Inden personale hos myndigheder med adgangsret til SIS får tilladelse til at behandle oplysninger, der er lagret i SIS, og periodisk efter at der er givet adgang til SIS-oplysninger, skal det modtage relevant uddannelse vedrørende datasikkerhed, grundlæggende rettigheder, herunder databeskyttelsesregler, og reglerne og procedurerne for databehandling som fastsat i SIRENE-håndbogen. Personalet oplyses om relevante bestemmelser om strafbare handlinger og strafferetlige sanktioner, herunder dem, der er fastsat i artikel 59.

2. Medlemsstaterne skal have et nationalt SIS-uddannelsesprogram, som skal omfatte uddannelse for såvel slutbrugere som SIRENE-kontorernes personale.

   Dette uddannelsesprogram kan være en del af et generelt uddannelsesprogram på nationalt plan, der omfatter uddannelse på andre relevante områder.

3. Fælles uddannelseskurser skal tilrettelægges på EU-plan mindst én gang om året for at styrke samarbejdet mellem SIRENE-kontorerne.

Kapitel III
eu-LISA's ansvar

Artikel 15

Operationel forvaltning

1. eu-LISA er ansvarligt for den operationelle forvaltning af det centrale SIS. eu-LISA sikrer i samarbejde med medlemsstaterne og med forbehold af en cost-benefit-analyse, at den bedst tilgængelige teknologi til enhver tid anvendes til det centrale SIS.

2. eu-LISA er også ansvarligt for følgende opgaver i forbindelse med kommunikationsinfrastrukturen:

   a) tilsyn

   b) sikkerhed

   c) koordinering af forbindelserne mellem medlemsstaterne og leverandøren

   d) opgaver i forbindelse med budgetgennemførelsen

   e) anskaffelse og fornyelse, og

   f) kontraktforhold.

3. eu-LISA er også ansvarligt for følgende opgaver vedrørende SIRENE-kontorerne og kommunikationen mellem SIRENE-kontorerne:

a) koordinering, styring af og støtte til testaktiviteter

b) opretholdelse og opdatering af tekniske specifikationer for udveksling af supplerende oplysninger mellem SIRENE-kontorerne og kommunikationsinfrastrukturen, og

c) håndtering af konsekvenserne af tekniske ændringer, hvor disse påvirker både SIS og udvekslingen af supplerende oplysninger mellem SIRENE-kontorerne.

4. eu-LISA udvikler og opretholder en mekanisme og en række procedurer til udførelse af kvalitetskontrol af oplysningerne i CS-SIS. Det forelægger regelmæssigt medlemsstaterne rapporter i denne henseende.

eu-LISA forelægger regelmæssigt Kommissionen en rapport vedrørende de konstaterede problemer og de berørte medlemsstater.

Kommissionen forelægger regelmæssigt Europa-Parlamentet og Rådet en rapport vedrørende datakvalitetsproblemer, der konstateres.

5. eu-LISA varetager også opgaver vedrørende uddannelse i den tekniske anvendelse af SIS og vedrørende foranstaltninger til forbedring af SIS-oplysningernes kvalitet.

6. Den operationelle forvaltning af det centrale SIS omfatter alle de opgaver, der er nødvendige for, at det centrale SIS kan fungere døgnet rundt alle ugens dage i overensstemmelse med denne forordning, navnlig den vedligeholdelse og den tekniske udvikling, der er nødvendig for, at systemet kan fungere gnidningsløst. Disse opgaver omfatter også koordinering og styring af samt støtte til testaktiviteter for det centrale SIS og N.SIS, der sikrer, at det centrale SIS og N.SIS fungerer i overensstemmelse med kravene til teknisk og funktionel overensstemmelse fastsat i artikel 9.

7. Kommissionen vedtager gennemførelsesretsakter med henblik på fastsættelse af de tekniske krav til kommunikationsinfrastrukturen. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

Artikel 16

Sikkerhed – eu-LISA

1. eu-LISA træffer de nødvendige foranstaltninger, herunder en sikkerhedsplan, en driftskontinuitetsplan og en katastrofeberedskabsplan, for det centrale SIS og kommunikationsinfrastrukturen, med henblik på:

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

   b) at forhindre, at uautoriserede personer får adgang til de anlæg, der benyttes til behandling af personoplysninger (kontrol med fysisk adgang til anlæggene)

c) at forhindre uautoriseret læsning, kopiering, ændring eller sletning af datamedier (kontrol med datamedier)

d) at forhindre uautoriseret indlæsning af oplysninger samt uautoriseret læsning, ændring eller sletning af lagrede personoplysninger (kontrol med lagring)

e) at forhindre, at de automatiserede databehandlingssystemer kan benyttes af uautoriserede personer ved hjælp af datakommunikationsudstyr (brugerkontrol)

f) at forhindre uautoriseret behandling af oplysninger i SIS samt uautoriseret ændring eller sletning af oplysninger, der er behandlet i SIS (kontrol med dataindlæsning)

g) at sikre, at personer, der har tilladelse til at anvende et automatiseret databehandlingssystem, kun har adgang til de oplysninger, der er omfattet af deres adgangstilladelse, ved hjælp af individuelle og entydige brugeridentifikatorer og udelukkende fortrolige adgangstilstande (kontrol med adgang til oplysninger)

h) at oprette profiler, der beskriver funktioner og ansvarsområder for de personer, som har tilladelse til at få adgang til oplysningerne eller anlæggene, og straks stille disse profiler til rådighed for Den Europæiske Tilsynsførende for Databeskyttelse på dennes anmodning (personaleprofiler)

i) at sikre, at det er muligt at undersøge og fastslå, til hvilke myndigheder der kan videregives personoplysninger via datakommunikationsudstyr (kontrol med videregivelse)

j) at sikre, at det er muligt efterfølgende at undersøge og fastslå, hvilke personoplysninger der er indlæst i de automatiserede databehandlingssystemer, hvornår og af hvem (kontrol med indlæsning)

k) at forhindre uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger i forbindelse med videregivelse af personoplysninger eller under transport af datamedier, navnlig ved hjælp af hensigtsmæssige krypteringsteknikker (transportkontrol)

l) at kontrollere effektiviteten af de sikkerhedsforanstaltninger, der er omhandlet i dette stykke, og træffe de nødvendige organisatoriske foranstaltninger vedrørende intern kontrol for at sikre overholdelsen af denne forordning (egenkontrol)

m) at sikre, at installerede systemer i tilfælde af afbrudt drift kan genetableres til normal drift (genopretning)

n) at sikre, at SIS fungerer korrekt, at fejl rapporteres (pålidelighed), og at personoplysninger lagret i SIS ikke kan ødelægges ved hjælp af systemsvigt (integritet), og

o) at sørge for sikkerheden af sine tekniske anlæg.

2. eu-LISA træffer foranstaltninger svarende til dem, der er omhandlet i stk. 1, for så vidt angår sikkerhed i forbindelse med behandling og udveksling af supplerende oplysninger gennem kommunikationsinfrastrukturen.

Artikel 17

Fortrolighed – eu-LISA

1. eu-LISA anvender passende regler for tavshedspligt eller andre tilsvarende fortrolighedskrav af en standard svarende til dem, der er fastsat i denne forordnings artikel 11, i forhold til alt personale, der skal arbejde med SIS-oplysninger, jf. dog personalevedtægtens artikel 17. Denne pligt fortsætter med at bestå, efter at de pågældende personer er fratrådt deres stilling, eller deres virksomhed er ophørt.

2. eu-LISA træffer foranstaltninger svarende til dem, der er omhandlet i stk. 1, for så vidt angår fortrolighed i forbindelse med udveksling af supplerende oplysninger gennem kommunikationsinfrastrukturen.

3. Hvis eu-LISA samarbejder med eksterne kontrahenter i forbindelse med SIS-relaterede opgaver, skal eu-LISA nøje overvåge kontrahentens aktiviteter for at sikre overholdelsen af alle denne forordnings bestemmelser, navnlig med hensyn til sikkerhed, fortrolighed og databeskyttelse.

4. Den operationelle forvaltning af CS-SIS må ikke overdrages til private virksomheder eller private organisationer.

Artikel 18

Opbevaring af logfiler på centralt plan

1. eu-LISA påser, at enhver adgang til og alle udvekslinger af personoplysninger inden for CS-SIS registreres til formålene i artikel 12, stk. 1.

2. Logfilerne skal navnlig vise indberetningens hidtidige forløb, dato og tidspunkt for databehandlingen, de oplysninger, der er anvendt til en søgning, en henvisning til de oplysninger, der er behandlet, samt de individuelle og entydige brugeridentifikatorer for den kompetente myndighed, der behandler oplysningerne.

3. Hvis en søgning foretages med fingeraftryksoplysninger eller ansigtsbilleder, jf. artikel 33, skal logfilerne som en undtagelse fra nærværende artikels stk. 2 vise den type oplysninger, der er anvendt til søgningen, frem for de faktiske oplysninger.

4. Logfilerne må kun anvendes til de i stk. 1 omhandlede formål og slettes tre år efter deres oprettelse. De logfiler, der indeholder indberetningernes hidtidige forløb, slettes tre år efter, at indberetningerne er slettet.

5. Logfilerne kan opbevares længere end de perioder, der er omhandlet i stk. 4, hvis der er brug for dem i forbindelse med kontrolprocedurer, som allerede er indledt.

6. Med henblik på at udøve egenkontrol og sikre CS-SIS' korrekte funktion og dataintegritet og -sikkerhed har eu-LISA adgang til logfilerne inden for rammerne af sine beføjelser.

Den Europæiske Tilsynsførende for Databeskyttelse har på anmodning adgang til disse logfiler inden for rammerne af sine beføjelser og med henblik på at udføre sine opgaver.

Kapitel IV
Information til offentligheden

Artikel 19

SIS-informationskampagner

Når denne forordning begynder at finde anvendelse, gennemfører Kommissionen i samarbejde med tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse en kampagne for at oplyse offentligheden om formålene med SIS, de i SIS lagrede oplysninger, hvilke myndigheder der har adgang til SIS, og de registreredes rettigheder. Kommissionen gentager regelmæssigt sådanne kampagner i samarbejde med tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse. Kommissionen driver et websted, som offentligheden har adgang til, med al relevant information om SIS. Medlemsstaterne udformer og gennemfører i samarbejde med deres tilsynsmyndigheder de politikker, der er nødvendige for generelt at orientere deres borgere og indbyggere om SIS.

Kapitel V
Indberetninger om nægtelse af indrejse og ophold for tredjelandsstatsborgere

Artikel 20

Kategorier af oplysninger

1. SIS skal udelukkende indeholde de kategorier af oplysninger, der meddeles af hver medlemsstat, og som er nødvendige til de formål, der er fastsat i artikel 24 og 25, jf. dog artikel 8, stk. 1, eller denne forordnings bestemmelser vedrørende lagring af supplerende oplysninger.

2. Enhver indberetning i SIS, der indeholder oplysninger om personer, må kun omfatte følgende:

   a) efternavne

   b) fornavne

   c) fødenavne

   d) tidligere anvendte navne og kaldenavne

   e) særlige fysiske kendetegn af objektiv og blivende karakter

f) fødested

g) fødselsdato

h) køn

i) samtlige nationaliteter

j) hvorvidt den pågældende person:

   i) er bevæbnet

   ii) er voldelig

   iii) er forsvundet eller undveget

   iv) er selvmordstruet

   v) udgør en trussel mod den offentlige sundhed, eller

   vi) er involveret i en aktivitet som omhandlet i artikel 3-14 i direktiv (EU) 2017/541

k) indberetningsgrunden

l) den myndighed, der har oprettet indberetningen

m) en henvisning til den afgørelse, der ligger til grund for indberetningen

n) den handling, der skal foretages i tilfælde af et hit

o) sammenkobling med andre indberetninger, jf. artikel 48

p) om vedkommende er familiemedlem til en unionsborger eller en anden person, som er berettiget til fri bevægelighed som omhandlet i artikel 26

q) om afgørelsen om nægtelse af indrejse og ophold er baseret på:

   i) en tidligere dom, jf. artikel 24, stk. 2, litra a)

   ii) en alvorlig sikkerhedstrussel, jf. artikel 24, stk. 2, litra b)

   iii) en omgåelse af EU-retten eller national ret om indrejse og ophold, jf. artikel 24, stk. 2, litra c)

   iv) et indrejseforbud, jf. artikel 24, stk. 1, litra b), eller

   v) en restriktiv foranstaltning, jf. artikel 25

r) lovovertrædelsens art

s) arten af personens identifikationsdokumenter

t) det land, der har udstedt personens identifikationsdokumenter

u) nummeret/numrene på personens identifikationsdokumenter

v) datoen for udstedelsen af personens identifikationsdokumenter

w) fotografier og ansigtsbilleder

x) fingeraftryksoplysninger

y) en kopi af identifikationsdokumenterne, så vidt muligt i farver.

3. Kommissionen vedtager gennemførelsesretsakter med henblik på fastsættelse og udarbejdelse af de tekniske regler, der er nødvendige for at indlæse, ajourføre, slette og søge i de i denne artikels stk. 2 omhandlede oplysninger, samt de fælles standarder, der er omhandlet i denne artikels stk. 4. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

4. De tekniske regler skal være tilsvarende for søgninger i CS-SIS, i nationale eller delte kopier og i tekniske kopier udarbejdet i medfør af artikel 41, stk. 2. De skal være baseret på fælles standarder.

Artikel 21

Proportionalitet

1. Forud for indlæsning af en indberetning og ved forlængelse af en indberetnings gyldighedsperiode undersøger medlemsstaten, om sagen er egnet, relevant og vigtig nok til at retfærdiggøre en indberetning i SIS.

2. Hvis afgørelsen om nægtelse af indrejse og ophold som omhandlet i artikel 24, stk. 1, litra a), er knyttet til en terrorhandling, anses sagen for at være egnet, relevant og vigtig nok til at retfærdiggøre en indberetning i SIS. Af hensyn til den offentlige eller nationale sikkerhed kan medlemsstaterne undtagelsesvis undlade at indlæse en indberetning, når det er sandsynligt, at den vil hindre officielle eller retlige undersøgelser, efterforskninger eller procedurer.

Artikel 22

Krav til indlæsning af en indberetning

1. De minimumsoplysninger, der er nødvendige for at indlæse en indberetning i SIS, er de oplysninger, der er omhandlet i artikel 20, stk. 2, litra a), g), k), m), n) og q). De øvrige oplysninger omhandlet i nævnte stykke indlæses også i SIS, hvis de foreligger.

2. De oplysninger, der er omhandlet i denne forordnings artikel 20, stk. 2, litra e), indlæses kun, når dette er strengt nødvendigt for identifikation af den pågældende tredjelandsstatsborger. Når sådanne oplysninger indlæses, sikrer medlemsstaterne, at artikel 9 i forordning (EU) 2016/679 overholdes.

Artikel 23

Indberetningers kompatibilitet

1. Forud for indlæsning af en indberetning undersøger medlemsstaten, om der allerede findes en indberetning i SIS om den pågældende person. Med henblik herpå foretages der også en sammenligning med fingeraftryksoplysninger, hvis sådanne oplysninger er til rådighed.

2. Der må kun indlæses én indberetning i SIS pr. person pr. medlemsstat. Hvis det er nødvendigt, kan nye indberetninger om samme person indlæses af andre medlemsstater i overensstemmelse med stk. 3.

3. Når der allerede findes en indberetning i SIS om en given person, kontrollerer den medlemsstat, der ønsker at indlæse en ny indberetning, at indberetningerne er kompatible. Hvis de er kompatible, kan medlemsstaten indlæse den nye indberetning. Hvis indberetningerne ikke er kompatible, konsulterer de berørte medlemsstaters SIRENE-kontorer hinanden via udveksling af supplerende oplysninger med henblik på nå frem til en aftale. Reglerne om indberetningers kompatibilitet fastsættes i SIRENE-håndbogen. Reglerne om kompatibilitet kan fraviges efter konsultationer mellem medlemsstaterne, hvis vigtige nationale interesser kræver det.

4. I tilfælde af hit på flere indberetninger om samme person, overholder den fuldbyrdende medlemsstat de regler om indberetningers prioritet, der er fastsat i SIRENE-håndbogen.

Hvis en person er omfattet af flere indberetninger indlæst af forskellige medlemsstater, fuldbyrdes indberetninger om anholdelse, der er indlæst i overensstemmelse med artikel 26 i forordning (EU) 2018/…[+], som en prioritet, jf. nævnte forordnings artikel 25.

Artikel 24

Betingelser for at indlæse indberetninger om nægtelse af indrejse og ophold

1. Medlemsstaterne indlæser en indberetning om nægtelse af indrejse og ophold, når en af følgende betingelser er opfyldt:

a) medlemsstaten har på grundlag af en individuel vurdering, som omfatter en vurdering af den pågældende tredjelandsstatsborgers personlige omstændigheder og konsekvenserne af at nægte vedkommende indrejse og ophold, konkluderet, at tilstedeværelsen af nævnte tredjelandsstatsborger på dens område udgør en trussel mod den offentlige orden, den offentlige sikkerhed eller den nationale sikkerhed, og medlemsstaten har derfor vedtaget en retlig eller administrativ afgørelse i overensstemmelse med sin nationale ret om at nægte indrejse og ophold og foretaget en national indberetning med henblik på nægtelse af indrejse og ophold, eller

b) medlemsstaten har udstedt et indrejseforbud over for en tredjelandsstatsborger i overensstemmelse med procedurer, der overholder direktiv 2008/115/EF.

[+] EUT: Indsæt venligst nummeret på forordningen i PE-CONS 36/18.

2. De situationer, der er omfattet af stk. 1, litra a), opstår, når

a) en tredjelandsstatsborger i en medlemsstat er blevet dømt for en lovovertrædelse, for hvilken en frihedsstraf af en varighed på mindst et år er foreskrevet

b) der er begrundet mistanke om, at en tredjelandsstatsborger har begået en grov strafbar handling, herunder en terrorhandling, eller der er tydelige tegn på, at den pågældende har til hensigt at begå en sådan strafbar handling på en medlemsstats område, eller

c) en tredjelandsstatsborger har omgået eller forsøgt at omgå EU-retten eller national ret om indrejse til og ophold på medlemsstaternes område.

3. Den indberettende medlemsstat sikrer, at indberetningen får virkning i SIS, så snart den pågældende tredjelandsstatsborger har forladt medlemsstaternes område, eller så snart som muligt, hvis den indberettende medlemsstat har fået tydelige tegn på, at tredjelandsstatsborgeren har forladt medlemsstaternes område, med henblik på at forhindre, at denne tredjelandsstatsborger rejser ind igen.

4. Personer, over for hvem der er truffet en afgørelse om nægtelse af indrejse og ophold, jf. stk. 1, har ret til at påklage afgørelsen. Sådanne klagesager behandles i overensstemmelse med EU-retten og national ret og skal omfatte et effektivt retsmiddel ved en domstol.

Artikel 25

Betingelser for at indlæse indberetninger om tredjelandsstatsborgere, som er omfattet af restriktive foranstaltninger

1. Indberetninger vedrørende tredjelandsstatsborgere, som er omfattet af restriktive foranstaltninger, der skal forhindre indrejse i eller transit gennem medlemsstaternes område, og som er truffet i overensstemmelse med retsakter, der er vedtaget af Rådet, herunder foranstaltninger til gennemførelse af et rejseforbud udstedt af De Forenede Nationers Sikkerhedsråd, indlæses i det omfang, at datakvalitetskravene er opfyldt, i SIS med henblik på nægtelse af indrejse og ophold.

2. Indberetningerne indlæses, ajourføres og slettes af den kompetente myndighed i den medlemsstat, der har formandskabet for Rådet for Den Europæiske Union på tidspunktet for foranstaltningens vedtagelse. Hvis denne medlemsstat ikke har adgang til SIS eller til indberetninger indlæst i overensstemmelse med denne forordning, påhviler ansvaret den medlemsstat, der har det efterfølgende formandskab, og som har adgang til SIS, herunder indberetninger indlæst i overensstemmelse med denne forordning.

   Medlemsstaterne indfører de procedurer, der er nødvendige for at indlæse, ajourføre og slette sådanne indberetninger.

Artikel 26

Betingelser for at indlæse indberetninger om tredjelandsstatsborgere, som er berettiget til fri bevægelighed inden for Unionen

1. En indberetning vedrørende en tredjelandsstatsborger, som er berettiget til fri bevægelighed inden for Unionen i overensstemmelse med direktiv 2004/38/EF eller med til en aftale mellem Unionen eller Unionen og dens medlemsstater på den ene side og et tredjeland på den anden side skal være i overensstemmelse med de regler, der er vedtaget til gennemførelse af nævnte direktiv eller aftale.

2. I tilfælde af et hit på en indberetning indlæst i overensstemmelse med artikel 24 vedrørende en tredjelandsstatsborger, som er berettiget til fri bevægelighed inden for Unionen, konsulterer den fuldbyrdende medlemsstat omgående den indberettende medlemsstat via udveksling af supplerende oplysninger, for at der straks kan træffes afgørelse om, hvilke handlinger der skal foretages.

Artikel 27

Konsultation forud for udstedelse eller forlængelse

af en opholdstilladelse eller et visum til længerevarende ophold

Hvis en medlemsstat overvejer at udstede eller forlænge en opholdstilladelse eller et visum til længerevarende ophold til en tredjelandsstatsborger, som er genstand for en indberetning om nægtelse af indrejse og ophold, der er indlæst af en anden medlemsstat, konsulterer de berørte medlemsstater hinanden ved udveksling af supplerende oplysninger i overensstemmelse med følgende regler:

a) den udstedende medlemsstat konsulterer den indberettende medlemsstat, før den udsteder eller forlænger opholdstilladelsen eller visummet til længerevarende ophold

b) den indberettende medlemsstat svarer på anmodningen om konsultation inden for ti kalenderdage

c) svares der ikke inden for den frist, der er omhandlet i litra b), betyder det, at den indberettende medlemsstat ikke gør indsigelse mod udstedelsen eller forlængelsen af opholdstilladelsen eller visummet til længerevarende ophold

d) når den udstedende medlemsstat træffer den relevante afgørelse, tager den hensyn til begrundelserne for den indberettende medlemsstats afgørelse og overvejer i overensstemmelse med national ret enhver trussel mod den offentlige orden eller offentlige sikkerhed, som den pågældende tredjelandsstatsborgers tilstedeværelse på medlemsstaternes område kan udgøre

e) den udstedende medlemsstat underretter den indberettende medlemsstat om sin afgørelse, og

f) hvis den udstedende medlemsstat underretter den indberettende medlemsstat om, at den har til hensigt at udstede eller forlænge opholdstilladelsen eller visummet til længerevarende ophold, eller at den har besluttet at gøre det, sletter den indberettende medlemsstat indberetningen om nægtelse af indrejse og ophold.

Den endelige afgørelse om, hvorvidt der skal udstedes en opholdstilladelse eller et visum til længerevarende ophold til en tredjelandsstatsborger, påhviler den udstedende medlemsstat.

Artikel 28

Konsultation forud for indlæsning af en indberetning om nægtelse af indrejse og ophold

Hvis en medlemsstat har truffet en afgørelse som omhandlet i artikel 24, stk. 1, og overvejer at indlæse en indberetning om nægtelse af indrejse og ophold vedrørende en tredjelandsstatsborger, som er indehaver af en gyldig opholdstilladelse eller et gyldigt visum til længerevarende ophold, som er udstedt af en anden medlemsstat, konsulterer de berørte medlemsstater hinanden ved udveksling af supplerende oplysninger i overensstemmelse med følgende regler:

a) den medlemsstat, der har truffet den afgørelse, der er omhandlet i artikel 24, stk. 1, underretter den udstedende medlemsstat om afgørelsen

b) de oplysninger, der er udvekslet i medfør af denne artikels litra a), skal indeholde tilstrækkelig information om begrundelserne for den afgørelse, der er omhandlet i artikel 24, stk. 1

c) på grundlag af oplysningerne fra den medlemsstat, der har truffet den afgørelse, der er omhandlet i artikel 24, stk. 1, overvejer den udstedende medlemsstat, om der er grund til at inddrage opholdstilladelsen eller visummet til længerevarende ophold

d) når den udstedende medlemsstat træffer den relevante afgørelse, tager den hensyn til begrundelserne for afgørelsen som angivet af den medlemsstat, der har truffet den afgørelse, der er omhandlet i artikel 24, stk. 1, og overvejer i overensstemmelse med national ret enhver trussel mod den offentlige orden eller offentlige sikkerhed, som den pågældende tredjelandsstatsborgers tilstedeværelse på medlemsstaternes område kan udgøre

e) senest 14 kalenderdage efter modtagelsen af anmodningen om konsultation underretter den udstedende medlemsstat den medlemsstat, der har truffet den afgørelse, der er omhandlet i artikel 24, stk. 1, om sin afgørelse eller indgiver, hvis det har været umuligt for den udstedende medlemsstat at træffe en afgørelse inden for denne frist, en begrundet anmodning om undtagelsesvis at forlænge fristen for sit svar med højst yderligere 12 kalenderdage

f) hvis den udstedende medlemsstat underretter den medlemsstat, der har truffet den afgørelse, der er omhandlet i artikel 24, stk. 1, om, at den fastholder opholdstilladelsen eller visummet til længerevarende ophold, indlæser den medlemsstat, der har truffet afgørelsen, ikke indberetning om nægtelse af indrejse og ophold.

Artikel 29

Konsultation efter indlæsning af en indberetning

om nægtelse af indrejse og ophold

Hvis det viser sig, at en medlemsstat har indlæst en indberetning om nægtelse af indrejse og ophold vedrørende en tredjelandsstatsborger, som er indehaver af en gyldig opholdstilladelse eller et gyldigt visum til længerevarende ophold, som er udstedt af en anden medlemsstat, konsulterer de berørte medlemsstater hinanden ved udveksling af supplerende oplysninger i overensstemmelse med følgende regler:

a) den indberettende medlemsstat underretter den udstedende medlemsstat om indberetningen om nægtelse af indrejse og ophold

b) de oplysninger, der udveksles i medfør af litra a), skal indeholde tilstrækkelig information om begrundelserne for indberetningen om nægtelse af indrejse og ophold

c) på grundlag af oplysningerne fra den indberettende medlemsstat overvejer den udstedende medlemsstat, om der er grund til at inddrage opholdstilladelsen eller visummet til længerevarende ophold

d) når den udstedende medlemsstat træffer sin afgørelse, tager den hensyn til den indberettende medlemsstats begrundelser for afgørelsen og overvejer i overensstemmelse med national ret enhver trussel mod den offentlige orden eller offentlige sikkerhed, som den pågældende tredjelandsstatsborgers tilstedeværelse på medlemsstaternes område kan udgøre

e) senest 14 kalenderdage efter modtagelsen af anmodningen om konsultation underretter den udstedende medlemsstat den indberettende medlemsstat om sin afgørelse, eller indgiver, hvis det ha været umuligt for den udstedende medlemsstat at træffe en afgørelse inden for denne frist, en begrundet anmodning om undtagelsesvis at forlænge fristen for sit svar med højst yderligere 12 kalenderdage

f) hvis den udstedende medlemsstat underretter den indberettende medlemsstat om, at den fastholder opholdstilladelsen eller visummet til længerevarende ophold, sletter den indberettende medlemsstat omgående indberetningen om nægtelse af indrejse og ophold.

Artikel 30

Konsultation i tilfælde af et hit vedrørende en tredjelandsstatsborger, der er indehaver af en gyldig opholdstilladelse eller et gyldigt visum til længerevarende ophold

Hvis en medlemsstat får et hit på en indberetning om nægtelse af indrejse og ophold indlæst af en medlemsstat vedrørende en tredjelandsstatsborger, der er indehaver af en gyldig opholdstilladelse eller et gyldigt visum til længerevarende ophold udstedt af en anden medlemsstat, konsulterer de involverede medlemsstater hinanden ved udveksling af supplerende oplysninger i overensstemmelse med følgende regler:

a) den fuldbyrdende medlemsstat underretter den indberettende medlemsstat om situationen

b) den indberettende medlemsstat indleder proceduren i artikel 29

c) den indberettende medlemsstat underretter den fuldbyrdende medlemsstat om resultatet af konsultationen.

Afgørelsen om den pågældende tredjelandsstatsborgers indrejse træffes af den fuldbyrdende medlemsstat i overensstemmelse med forordning (EU) 2016/399.

Artikel 31

Statistikker om udveksling af oplysninger

Medlemsstaterne forelægger på årlig basis eu-LISA statistikker om de udvekslinger af oplysninger, der er gennemført i overensstemmelse med artikel 27-30, og om de tilfælde, hvor fristerne i de nævnte artikler ikke blev overholdt.

Kapitel VI
Søgning med biometriske data

Artikel 32

Særlige regler for indlæsning af fotografier, ansigtsbilleder og fingeraftryksoplysninger

1. Kun de i artikel 20, stk. 2, litra w) og x), omhandlede fotografier, ansigtsbilleder og fingeraftryksoplysninger, der opfylder minimumsstandarder for datakvalitet og tekniske specifikationer, må indlæses i SIS. Før disse oplysninger indlæses, skal der udføres en kvalitetskontrol for at fastslå, om minimumsstandarderne for datakvalitet og de tekniske specifikationer er opfyldt.

2. Fingeraftryksoplysninger, der indlæses i SIS, kan bestå af et til ti flade fingeraftryk og et til ti rullede fingeraftryk. De kan også omfatte op til to håndfladeaftryk.

3. Minimumsstandarder for datakvalitet og tekniske specifikationer for lagring af de biometriske data, der er omhandlet i denne artikels stk. 1, fastsættes i overensstemmelse med denne artikels stk. 4. Disse minimumsstandarder for datakvalitet og tekniske specifikationer fastsætter det kvalitetsniveau, der kræves for at anvende oplysningerne til at kontrollere identiteten af en person i henhold til artikel 33, stk. 1, og for at anvende oplysningerne til at identificere en person i overensstemmelse med artikel 33, stk. 2-4.

4. Kommissionen vedtager gennemførelsesretsakter med henblik på fastsættelse af de minimumsstandarder for datakvalitet og tekniske specifikationer, der er omhandlet i denne artikels stk. 1 og 3. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

Artikel 33

Særlige regler for kontrol eller søgning med fotografier, ansigtsbilleder og fingeraftryksoplysninger

1. Når en indberetning i SIS indeholder fotografier, ansigtsbilleder og fingeraftryksoplysninger, anvendes sådanne fotografier, ansigtsbilleder og fingeraftryksoplysninger til at bekræfte identiteten på en person, der er lokaliseret som følge af en alfanumerisk søgning i SIS.

2. Der kan i alle tilfælde søges på fingeraftryksoplysninger for at identificere en person. Der skal dog søges på fingeraftryksoplysninger for at identificere en person, hvor en persons identitet ikke kan fastslås på anden måde Med henblik herpå skal det centrale SIS omfatte et automatisk fingeraftryksidentifikationssystem (AFIS).

3. Der kan også søges på fingeraftryksoplysninger i SIS i forbindelse med indberetninger, der er indlæst i overensstemmelse med artikel 24 og 25, ved anvendelse af fuldstændige eller ufuldstændige sæt af fingeraftryk eller håndfladeaftryk, der er fundet på et gerningssted under efterforskning af grov kriminalitet eller terrorhandlinger, hvor det med en høj grad af sandsynlighed kan fastslås, at disse sæt af aftryk tilhører en gerningsmand, og såfremt søgningen foretages samtidigt i medlemsstatens relevante nationale fingeraftryksdatabaser.

4. Så snart det bliver teknisk muligt, og idet der samtidig skal sikres en meget pålidelig identifikation, kan fotografier og ansigtsbilleder anvendes til at identificere en person i forbindelse med almindelige grænseovergangssteder.

Inden funktionen implementeres i SIS, fremlægger Kommissionen en rapport om den nødvendige teknologis tilgængelighed, umiddelbare anvendelighed og pålidelighed. Europa-Parlamentet høres om rapporten.

Efter at funktionen er taget i brug ved almindelige grænseovergangssteder, tillægges Kommissionen beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 61 for at supplere denne forordning vedrørende fastlæggelsen af, under hvilke andre omstændigheder fotografier og ansigtsbilleder kan anvendes til at identificere personer.

Kapitel VII

Adgangsret og undersøgelse og sletning af indberetninger

Artikel 34

Nationale kompetente myndigheder med adgangsret til oplysninger i SIS

1. Nationale kompetente myndigheder med ansvar for identifikation af tredjelandsstatsborgere har adgang til oplysninger, der er indlæst i SIS, og ret til at søge direkte i disse oplysninger eller i en kopi af SIS-databasen med henblik på:

   a) grænsekontrol i overensstemmelse med forordning (EU) 2016/399

   b) politi- og toldkontrol udført i den berørte medlemsstat og de udpegede myndigheders koordinering af sådan kontrol

   c) forebyggelse, afsløring, efterforskning eller retsforfølgning af terrorhandlinger eller andre alvorlige strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner i den berørte medlemsstat, forudsat at direktiv (EU) 2016/680 finder anvendelse

d) undersøgelse af betingelserne for og beslutningstagning vedrørende tredjelandsstatsborgeres indrejse og ophold på medlemsstaternes område, herunder vedrørende opholdstilladelser og visa til længerevarende ophold og tilbagesendelse af tredjelandsstatsborgere samt udførelse af kontrol af tredjelandsstatsborgere, der indrejser eller opholder sig ulovligt på medlemsstaternes område

e) sikkerhedskontrol af tredjelandsstatsborgere, der ansøger om international beskyttelse, for så vidt de myndigheder, der foretager kontrollerne, ikke er "besluttende myndigheder" som defineret i artikel 2, litra f), i Europa-Parlamentets og Rådets direktiv 2013/32/EU[1], og, hvor det er relevant, ydelse af rådgivning i overensstemmelse med Rådets forordning (EF) nr. 377/2004[2]

f) behandling af visumansøgninger og beslutningstagning vedrørende disse, herunder om visa skal annulleres, inddrages eller forlænges, jf. Europa-Parlamentets og Rådets forordning (EF) nr. 810/2009[3].

---

1 Europa-Parlamentets og Rådets direktiv 2013/32/EU af 26. juni 2013 om fælles procedurer for tildeling og fratagelse af international beskyttelse (EUT L 180 af 29.6.2013, s. 60).

2 Rådets forordning (EF) nr. 377/2004 af 19. februar 2004 om oprettelse af et netværk af indvandringsforbindelsesofficerer (EUT L 64 af 2.3.2004, s. 1).

3 Europa-Parlamentets og Rådets forordning (EF) nr. 810/2009 af 13. juli 2009 om en fællesskabskodeks for visa (visumkodeks) (EUT L 243 af 15.9.2009, s. 1).

2. Adgangsret til oplysninger i SIS og ret til at søge direkte i disse oplysninger kan udøves af nationale kompetente myndigheder med ansvar for naturalisation med henblik på behandling af en ansøgning om naturalisation som fastsat i national ret.

3. Med henblik på artikel 24 og 25 kan adgangsret til oplysninger i SIS og ret til at søge direkte i disse oplysninger også udøves af nationale judicielle myndigheder, herunder myndigheder med ansvar for indledning af offentlig retsforfølgning i straffesager og retlig efterforskning inden tiltale af en person, i forbindelse med varetagelsen af deres opgaver som fastsat i national ret og af deres koordinerende myndigheder.

4. Adgangsret til oplysninger om dokumenter vedrørende personer, der er indlæst i overensstemmelse med artikel 38, stk. 2, litra k) og l), i forordning (EU) 2018/…[+], og ret til at søge i disse oplysninger kan også udøves af de i denne artikels stk. 1, litra f), omhandlede myndigheder.

5. De kompetente myndigheder, der er omhandlet i denne artikel, medtages på den liste, der er omhandlet i artikel 41, stk. 8.

[+] EUT: Indsæt venligst nummeret på forordningen i PE-CONS 36/18.

Artikel 35

Europols adgang til oplysninger i SIS

1. Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol), der er oprettet ved forordning (EU) 2016/794, har, hvor det er nødvendigt for at opfylde dets mandat, ret til at tilgå og søge i oplysninger i SIS. Europol kan også udveksle og anmode om yderligere supplerende oplysninger i overensstemmelse med bestemmelserne i SIRENE-håndbogen.

2. Hvis en søgning foretaget af Europol viser, at der findes en indberetning i SIS, underretter Europol den indberettende medlemsstat via udveksling af supplerende oplysninger ved hjælp af kommunikationsinfrastrukturen og i overensstemmelse med SIRENE-håndbogens bestemmelser. Indtil Europol bliver i stand til at anvende de funktioner, der er beregnet til udveksling af supplerende oplysninger, underretter Europol den indberettende medlemsstat ad de kanaler, der er fastlagt i forordning (EU) 2016/794.

3. Europol må behandle de supplerende oplysninger, der er blevet fremsendt til det af medlemsstaterne, med henblik på at sammenligne dem med sine databaser og operationelle analyseprojekter for at finde sammenhænge eller andre relevante forbindelser og til strategiske, tematiske eller operationelle analyser som omhandlet i artikel 18, stk. 2, litra a), b) og c), i forordning (EU) 2016/794. Enhver behandling af supplerende oplysninger foretaget af Europol med henblik på nærværende artikel skal udføres i overensstemmelse med nævnte forordning.

4. Europols brug af oplysninger, der er tilvejebragt gennem søgning i SIS eller gennem behandling af supplerende oplysninger, kan kun finde sted med den indberettende medlemsstats samtykke. Hvis medlemsstaten giver tilladelse til at benytte sådanne oplysninger, skal Europols behandling heraf finde sted i overensstemmelse med forordning (EU) 2016/794. Europol må kun meddele tredjelande og eksterne organisationer sådanne oplysninger med den indberettende medlemsstats samtykke og under fuld overholdelse af EU-retten om databeskyttelse.

5. Europol:

a) må ikke tilslutte dele af SIS eller overføre de deri indeholdte oplysninger, som det har adgang til, til et system til dataindsamling og databehandling, der forvaltes af eller i Europol, eller downloade eller på anden måde kopiere nogen del af SIS, jf. dog stk. 4 og 6

b) sletter uanset artikel 31, stk. 1, i forordning (EU) 2016/794 supplerende oplysninger, der indeholder personoplysninger, senest et år efter, at den pågældende indberetning er blevet slettet. Som en undtagelse kan Europol, hvis det har oplysninger i sine databaser eller operationelle analyseprojekter om en sag, som de supplerende oplysninger vedrører, for at kunne udføre sine opgaver undtagelsesvis fortsat lagre de supplerende oplysninger, hvis det er nødvendigt. Europol underretter den indberettende og den fuldbyrdende medlemsstat om den fortsatte lagring af sådanne supplerende oplysninger og angiver begrundelsen herfor

c) begrænser adgangen til oplysninger i SIS, herunder supplerende oplysninger, til særligt bemyndiget Europolpersonale, der har brug for adgang til sådanne oplysninger for at kunne udføre sine opgaver

d) vedtager og anvender foranstaltninger for at garantere sikkerhed, fortrolighed og egenkontrol i overensstemmelse med artikel 10, 11 og 13

e) sikrer, at det personale, der er bemyndiget til at behandle SIS-oplysninger, modtager relevant uddannelse og relevante oplysninger i overensstemmelse med artikel 14, stk. 1, og

f) tillader Den Europæiske Tilsynsførende for Databeskyttelse at overvåge og undersøge Europols virksomhed, når det udøver sin ret til at tilgå og søge i oplysninger i SIS og udveksler og behandler supplerende oplysninger, jf. dog forordning (EU) 2016/794.

6. Europol må kun kopiere oplysninger fra SIS til tekniske formål, hvor dette er nødvendigt for, at behørigt bemyndiget Europolpersonale kan foretage en direkte søgning. Denne forordning finder anvendelse på sådanne kopier. Den tekniske kopi må kun anvendes til at lagre SIS-oplysninger, mens der søges i disse oplysninger. Når der er søgt i oplysningerne, skal de slettes. En sådan anvendelse betragtes ikke som ulovlig download eller kopiering af SIS-oplysninger. Europol må ikke kopiere indberetningsoplysninger eller uddybende oplysninger fra medlemsstaterne eller CS-SIS til andre Europolsystemer.

7. Med henblik på at kontrollere lovligheden af databehandling, udøve egenkontrol og sikre ordentlig datasikkerhed og -integritet gemmer Europol logfiler for hver adgang til og søgning i SIS i overensstemmelse med bestemmelserne i artikel 12. Disse logfiler og denne dokumentation betragtes ikke som ulovlig download eller kopiering af en del af SIS.

8. Medlemsstaterne underretter ved udveksling af supplerende oplysninger Europol om eventuelle hit på indberetninger i forbindelse med terrorhandlinger. Medlemsstaterne kan undtagelsesvis undlade at underrette Europol, hvis dette ville bringe igangværende efterforskninger eller en fysisk persons sikkerhed i fare eller være i strid med væsentlige sikkerhedsinteresser i den indberettende medlemsstat.

9. Stk. 8 finder anvendelse fra den dato, hvor Europol er i stand til at modtage supplerende oplysninger i overensstemmelse med stk. 1.

Artikel 36

Adgang til oplysninger i SIS for europæiske grænse- og kystvagthold, hold af medarbejdere, der er involveret i tilbagesendelsesrelaterede opgaver, og medlemmerne af migrationsstyringsstøtteholdene

1. I overensstemmelse med artikel 40, stk. 8, i forordning (EU) 2016/1624 har holdmedlemmerne som omhandlet i artikel 2, nr. 8) og 9), i nævnte forordning inden for deres mandat, og forudsat at de har tilladelse til at foretage kontrol i henhold til nærværende forordnings artikel 34, stk. 1, og har fået den nødvendige uddannelse i henhold til nærværende forordnings artikel 14, stk. 1, ret til at tilgå og søge i oplysninger i SIS, for så vidt det er nødvendigt for udførelsen af deres opgave, og som krævet i den operative plan for en specifik operation. Adgang til oplysninger i SIS må ikke udvides til også at omfatte andre holdmedlemmer.

2. De i stk. 1 omhandlede holdmedlemmer udøver retten til at tilgå og søge i oplysningerne i SIS, jf. stk. 1, via en teknisk grænseflade. Den tekniske grænseflade oprettes og vedligeholdes af Det Europæiske Agentur for Grænse- og Kystbevogtning og sikrer en direkte forbindelse til det centrale SIS.

3. Hvis en søgning foretaget af et af de i denne artikels stk. 1 omhandlede holdmedlemmer viser, at der findes en indberetning i SIS, underrettes den indberettende medlemsstat herom. I overensstemmelse med artikel 40 i forordning (EU) 2016/1624 må holdmedlemmerne kun reagere på en indberetning i SIS i henhold til instrukserne fra, og som hovedregel under tilstedeværelse af, grænsevagter eller medarbejdere, der er involveret i tilbagesendelsesrelaterede opgaver, fra den værtsmedlemsstat, som de opererer i. Værtsmedlemsstaten kan bemyndige holdmedlemmerne til at handle på sine vegne.

4. Med henblik på at kontrollere lovligheden af databehandling, udøve egenkontrol og sikre ordentlig datasikkerhed og -integritet gemmer Det Europæiske Agentur for Grænse- og Kystbevogtning logfiler for hver adgang til og søgning i SIS i overensstemmelse med bestemmelserne i artikel 12.

5. Det Europæiske Agentur for Grænse- og Kystbevogtning vedtager og anvender foranstaltninger for at garantere sikkerhed, fortrolighed og egenkontrol i overensstemmelse med artikel 10, 11 og 13 og sikrer, at de i nærværende artikels stk. 1 omhandlede hold anvender disse foranstaltninger.

6. Intet i denne artikel må fortolkes som en indskrænkning af bestemmelserne i forordning (EU) 2016/1624 om databeskyttelse eller Det Europæiske Agentur for Grænse- og Kystbevogtnings ansvar for dets uautoriserede eller forkerte behandling af oplysninger.

7. Med forbehold af stk. 2 må ingen dele af SIS tilsluttes et system til dataindsamling og databehandling, der forvaltes af de i stk. 1 omhandlede hold eller af Det Europæiske Agentur for Grænse- og Kystbevogtning, og ingen oplysninger i SIS, som disse hold har adgang til, må overføres til et sådant system. Ingen del af SIS må downloades eller kopieres. Logning af adgang og søgninger betragtes ikke som ulovlig download eller kopiering af SIS-oplysninger.

8. Det Europæiske Agentur for Grænse- og Kystbevogtning tillader Den Europæiske Tilsynsførende for Databeskyttelse at overvåge og undersøge de aktiviteter, der foretages af de i denne artikel omhandlede hold, når de udøver deres ret til at tilgå og søge i oplysninger i SIS. Dette berører ikke de yderligere bestemmelser i forordning (EU) 2018/…[+].

Artikel 37

Evaluering af Europols og

Det Europæiske Agentur for Grænse- og Kystbevogtnings anvendelse af SIS

1. Kommissionen foretager mindst hvert femte år en evaluering af driften og anvendelsen af SIS af Europol og de i artikel 36, stk. 1, omhandlede hold.

2. Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning sikrer en passende opfølgning på de resultater og henstillinger, som evalueringen afføder.

[+] EUT: Indsæt venligst nummeret på forordningen i PE-CONS 31/18.

3. En rapport om resultaterne af evalueringen og opfølgningen herpå sendes til Europa-Parlamentet og Rådet.

Artikel 38

Adgangens omfang

Slutbrugerne, herunder Europol og holdmedlemmerne som omhandlet i artikel 2, nr. 8) og 9), i forordning (EU) 2016/1624, må kun tilgå de oplysninger, der er nødvendige for varetagelsen af deres opgaver.

Artikel 39

Undersøgelsesfrist for indberetninger

1. Indberetninger opbevares kun så længe, det er nødvendigt af hensyn til de formål, der ligger til grund for indlæsningen.

2. En indberettende medlemsstat undersøger inden tre år efter, at den har indlæst indberetningen i SIS, behovet for fortsat at opbevare den. Hvis den nationale afgørelse, som indberetningen er baseret på, fastsætter en længere gyldighedsperiode end tre år, undersøges indberetningen dog inden for fem år.

3. Når det er passende, fastsætter hver enkelt medlemsstat kortere undersøgelsesfrister i overensstemmelse med national ret.

4. Inden udløbet af undersøgelsesfristen kan den indberettende medlemsstat efter en samlet individuel vurdering, der skal registreres, beslutte fortsat at opbevare indberetningen udover udløbet af undersøgelsesfristen, hvis det viser sig at være nødvendigt og forholdsmæssigt afpasset af hensyn til det formål, der ligger til grund for indlæsning af indberetningen. I så fald finder stk. 2 også anvendelse på forlængelsen af opbevaringsfristen. En sådan forlængelse meddeles CS-SIS.

5. Indberetninger slettes automatisk, når den i stk. 2 nævnte undersøgelsesfrist er udløbet, undtagen hvis den indberettende medlemsstat har meddelt CS-SIS en forlængelse, jf. stk. 4. CS-SIS underretter automatisk med fire måneders varsel den indberettende medlemsstat om en planlagt sletning af oplysninger.

6. Medlemsstaterne fører statistik over antallet af indberetninger, hvis opbevaringsfrist er blevet forlænget i overensstemmelse med denne artikels stk. 4, og fremsender dem på anmodning til de tilsynsmyndigheder, der er omhandlet i artikel 55.

7. Så snart det står klart for et SIRENE-kontor, at en indberetning om en person har opfyldt sit formål og derfor bør slettes, underretter det omgående den myndighed, som oprettede indberetningen. Myndigheden har 15 kalenderdage fra modtagelsen af denne underretning til at svare, at indberetningen er blevet eller vil blive slettet eller angive begrundelsen for, at indberetningen fortsat opbevares. Hvis der ikke modtages et svar inden for 15-dages-fristen, sikrer SIRENE-kontoret, at indberetningen slettes. Hvis det er tilladt i henhold til national ret, sletter SIRENE-kontoret indberetningen. SIRENE-kontorerne indberetter eventuelle gentagne problemer, som de støder på under udøvelse af dette stykke, til deres tilsynsmyndighed.

Artikel 40

Sletning af indberetninger

1. Indberetninger om nægtelse af indrejse og ophold i medfør af artikel 24 slettes:

   a) når den afgørelse, der lå til grund for at indlæse indberetningen, er blevet trukket tilbage eller annulleret af den kompetente myndighed, eller

   b) i givet fald på baggrund af den i artikel 27 og 29 omhandlede konsultationsprocedure.

2. Indberetninger om tredjelandsstatsborgere, som er omfattet af en restriktiv foranstaltning, der har til formål at forhindre indrejse i eller transit gennem medlemsstaternes område, slettes, når den restriktive foranstaltning er blevet ophævet, suspenderet eller annulleret.

3. Indberetninger om en person, som har opnået statsborgerskab i en medlemsstat eller en stat, hvis statsborgere er berettiget til fri bevægelighed i henhold til EU-retten, slettes, så snart den indberettende medlemsstat bliver klar over eller i medfør af artikel 44 er blevet underrettet om, at vedkommende har opnået et sådant statsborgerskab.

4. Indberetninger slettes ved indberetningens udløb i overensstemmelse med artikel 39.

Kapitel VIII

Generelle regler for behandling af oplysninger

Artikel 41

Behandling af SIS-oplysninger

1. Medlemsstaterne må kun behandle de oplysninger, der er omhandlet i artikel 20, med henblik på nægtelse af indrejse og ophold på deres områder.

2. Oplysningerne må kun kopieres til tekniske formål, hvor dette er nødvendigt for, at de kompetente myndigheder, der er omhandlet i artikel 34, kan foretage en direkte søgning. Denne forordning finder anvendelse på sådanne kopier. En medlemsstat må ikke kopiere indberetningsoplysninger eller uddybende oplysninger, som en anden medlemsstat har indlæst, fra sit N.SIS eller fra CS-SIS til andre nationale datafiler.

3. De i stk. 2 omhandlede tekniske kopier, som fører til offlinedatabaser, må højst eksistere i 48 timer.

   Uanset første afsnit er tekniske kopier, der fører til offlinedatabaser til brug for visumudstedende myndigheder, ikke tilladt, bortset fra kopier, som udelukkende oprettes til brug i en nødsituation, efter at netværket ikke har været tilgængeligt i mere end 24 timer.

Medlemsstaterne opbevarer en ajourført oversigt over disse kopier, stiller denne oversigt til rådighed for deres tilsynsmyndigheder, og sikrer, at denne forordning, navnlig artikel 10, anvendes på disse kopier.

4. Der må kun gives nationale kompetente myndigheder som omhandlet i artikel 34 adgang til oplysninger i SIS inden for rammerne af deres beføjelser og kun til behørigt autoriseret personale.

5. Medlemsstaterne må kun behandle SIS-oplysninger til andre formål end dem, hvortil de er indlæst i SIS, hvis der er en sammenhæng med en specifik sag, og hvis det er nødvendigt for at forebygge en overhængende og alvorlig trussel mod den offentlige orden og den offentlige sikkerhed, af tungtvejende hensyn til statens sikkerhed eller til forebyggelse af grov kriminalitet. I så fald skal der forinden indhentes tilladelse fra den indberettende medlemsstat med henblik herpå.

6. Oplysninger om dokumenter vedrørende personer, der er indlæst i SIS i medfør af artikel 38, stk. 2, litra k) og l), i forordning (EU) 2018/…[+], kan anvendes af de i artikel 34, stk. 1, litra f), omhandlede kompetente myndigheder i overensstemmelse med lovgivningen i den enkelte medlemsstat.

7. Enhver anvendelse af SIS-oplysninger i strid med denne artikels stk. 1-6 betragtes som misbrug i henhold til den enkelte medlemsstats nationale ret og er underlagt sanktioner i henhold til artikel 59.

[+] EUT: Indsæt venligst nummer på forordning PE-CONS 36/18.

8. Hver medlemsstat sender eu-LISA en liste over de af dets kompetente myndigheder, der har tilladelse til at søge i oplysningerne i SIS direkte i henhold til denne forordning, samt alle ændringer af denne liste. For hver myndighed på denne liste skal det angives, hvilke oplysninger den må søge i og til hvilke formål. eu-LISA sørger for, at listen offentliggøres i Den Europæiske Unions Tidende hvert år. eu-LISA fører på sit websted en liste, der løbende ajourføres, med de ændringer, som medlemsstaterne har indsendt imellem de årlige offentliggørelser.

9. For så vidt EU-retten ikke fastsætter særlige bestemmelser, finder den enkelte medlemsstats ret anvendelse på oplysningerne i dets N.SIS.

Artikel 42

SIS-oplysninger og nationale filer

1. Artikel 41, stk. 2, berører ikke en medlemsstats ret til i sine nationale filer at opbevare SIS-oplysninger, i forbindelse med hvilke der er foretaget handlinger på dens område. Sådanne oplysninger opbevares i nationale filer i højst tre år, medmindre der i national ret findes særlige bestemmelser om en længere opbevaringsfrist.

2. Artikel 41, stk. 2, berører ikke en medlemsstats ret til i nationale filer at opbevare oplysninger indeholdt i en bestemt indberetning, som den pågældende medlemsstat har indlæst i SIS.

Artikel 43

Oplysninger i tilfælde af manglende gennemførelse af en indberetning

Hvis en påkrævet handling ikke kan foretages, underretter den medlemsstat, der anmodes om at foretage handlingen, omgående den indberettende medlemsstat herom ved udveksling af supplerende oplysninger.

Artikel 44

Kvaliteten af oplysningerne i SIS

1. Den indberettende medlemsstat har ansvaret for at sikre, at oplysningerne er korrekte, ajourførte og lovligt indlæst og lagret i SIS.

2. Når en indberettende medlemsstat modtager relevante supplerende eller ændrede oplysninger som anført i artikel 20, stk. 2, færdiggør eller ændrer den straks den pågældende indberetning.

3. Kun den indberettende medlemsstat må ændre, supplere, rette, ajourføre eller slette de oplysninger, den har indlæst i SIS.

4. Hvis en anden medlemsstat end den indberettende medlemsstat har relevante supplerende eller ændrede oplysninger, jf. artikel 20, stk. 2, videregiver den dem straks ved udveksling af supplerende oplysninger til den indberettende medlemsstat, så denne kan færdiggøre eller ændre indberetningen. Oplysningerne videregives kun, hvis tredjelandsstatsborgerens identitet kan fastslås.

5. Hvis en anden medlemsstat end den indberettende medlemsstat er i besiddelse af dokumentation, der lader formode, at en oplysning er faktuelt ukorrekt eller er blevet lagret ulovligt, meddeler den ved udveksling af supplerende oplysninger den indberettende medlemsstat dette hurtigst muligt og senest to hverdage efter, at den fik kendskab til denne dokumentation. Den indberettende medlemsstat kontrollerer oplysningen og retter eller sletter om nødvendigt straks oplysningen.

6. Hvis medlemsstaterne ikke kan nå til enighed inden for to måneder efter, at dokumentationen blev kendt, jf. denne artikels stk. 5, forelægger den medlemsstat, der ikke har indlæst indberetningen, sagen for de berørte tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse med henblik på at få truffet en afgørelse ved hjælp af samarbejde i overensstemmelse med artikel 57.

7. Medlemsstaterne udveksler supplerende oplysninger, hvis en person klager over ikke at være den tiltænkte genstand for en indberetning. Hvis resultatet af undersøgelsen viser, at den tiltænkte genstand for en indberetning ikke er klageren, skal klageren underrettes om de i artikel 47 fastsatte foranstaltninger og om retten til retsmidler i medfør af artikel 54, stk. 1.

Artikel 45

Sikkerhedsrelaterede hændelser

1. Enhver hændelse, der har eller kan have indvirkning på sikkerheden i SIS eller kan forårsage beskadigelse eller tab af SIS-oplysninger eller af supplerende oplysninger, skal anses for at være en sikkerhedsrelateret hændelse, navnlig når ulovlig adgang til oplysninger kan have forekommet, eller hvor oplysningernes tilgængelighed, integritet og fortrolighed er eller kan være blevet kompromitteret.

2. Sikkerhedsrelaterede hændelser skal håndteres på en måde, der sikrer en hurtig, effektiv og passende reaktion.

3. Uden at det berører anmeldelsen af og underretningen om et brud på persondatasikkerheden, jf. artikel 33 i forordning (EU) 2016/679 eller artikel 30 i direktiv (EU) 2016/680, underretter medlemsstaterne, Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning straks Kommissionen, eu-LISA, den kompetente tilsynsmyndighed og Den Europæiske Tilsynsførende for Databeskyttelse om sikkerhedsrelaterede hændelser. eu-LISA underretter straks Kommissionen og Den Europæiske Tilsynsførende for Databeskyttelse om enhver sikkerhedsrelateret hændelse vedrørende det centrale SIS.

4. Oplysninger om en sikkerhedsrelateret hændelse, som har eller kan få indvirkning på driften af SIS i en medlemsstat eller i eu-LISA eller på tilgængeligheden, integriteten og fortroligheden af de oplysninger, der indlæses eller sendes af andre medlemsstater, eller de supplerende oplysninger, der udveksles, skal straks forelægges alle medlemsstaterne og indberettes i overensstemmelse med eu-LISA's hændelsesstyringsplan.

5. Medlemsstaterne og eu-LISA samarbejder i tilfælde af en sikkerhedsrelateret hændelse.

6. Kommissionen rapporterer omgående alvorlige hændelser til Europa-Parlamentet og Rådet. Disse rapporter klassificeres som RESTREINT UE/EU RESTRICTED i overensstemmelse med de gældende sikkerhedsregler.

7. Når en sikkerhedsrelateret hændelse er forårsaget af misbrug af oplysninger, sikrer medlemsstaterne, Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning, at der pålægges sanktioner i overensstemmelse med artikel 59.

Artikel 46

Sondring mellem personer med kendetegn, der ligner hinanden

1. Når det i forbindelse med indlæsning af en ny indberetning viser sig, at der allerede findes en indberetning i SIS om en person med samme identitetsbeskrivelse, tager SIRENE-kontoret inden for 12 timer kontakt til den indberettende medlemsstat ved udveksling af supplerende oplysninger for at undersøge, om genstandene for indberetningerne er samme person.

2. Hvis undersøgelsen viser, at genstanden for den nye indberetning og genstanden for den indberetning, der allerede er indlæst i SIS, faktisk er samme person, iværksætter SIRENE-kontoret den i artikel 23 omhandlede procedure for indlæsning af flere indberetninger.

3. Hvis undersøgelsen viser, at det faktisk drejer sig om to forskellige personer, godkender SIRENE-kontoret anmodningen om indlæsning af den anden indberetning ved at tilføje de nødvendige oplysninger for at forhindre fejlidentifikationer.

Artikel 47

Uddybende oplysninger med henblik på håndtering af identitetsmisbrug

1. Når der kan opstå forveksling mellem den person, der er den tiltænkte genstand for en indberetning, og en person, hvis identitet er blevet misbrugt, tilføjer den indberettende medlemsstat med udtrykkeligt samtykke fra den person, hvis identitet er blevet misbrugt, oplysninger vedrørende sidstnævnte i indberetningen for at undgå de negative følger af fejlidentifikation. Enhver person, hvis identitet er blevet misbrugt, har ret til at trække sit samtykke til behandling af de tilføjede personoplysninger tilbage.

2. Oplysninger vedrørende en person, hvis identitet er blevet misbrugt, må kun anvendes til følgende formål:

   a) at gøre det muligt for den kompetente myndighed at skelne mellem den person, hvis identitet er blevet misbrugt, og den person, der er den tiltænkte genstand for indberetningen, og

   b) at gøre det muligt for den person, hvis identitet er blevet misbrugt, at bevise sin identitet og fastslå, at vedkommendes identitet er blevet misbrugt.

3. Med henblik på denne artikel og med forbehold af et udtrykkeligt samtykke fra den person, hvis identitet er blevet misbrugt for hver enkelt datakategori, må kun følgende personoplysninger om en person, hvis identitet er blevet misbrugt, indlæses og viderebehandles i SIS:

a) efternavne

b) fornavne

c) fødenavne

d) tidligere anvendte navne og eventuelt særskilt indlæste kaldenavne

e) særlige fysiske kendetegn af objektiv og blivende karakter

f) fødested

g) fødselsdato

h) køn

i) fotografier og ansigtsbilleder

j) fingeraftryk, håndfladeaftryk eller begge

k) samtlige nationaliteter

l) arten af personens identifikationsdokumenter

m) det land, der har udstedt personens identifikationsdokumenter

n) nummeret/numrene på personens identifikationsdokumenter

o) datoen for udstedelse af personens identifikationsdokumenter

p) personens adresse

q) personens fars navn

r) personens mors navn.

4. Kommissionen vedtager gennemførelsesretsakter med henblik på fastsættelse og udarbejdelse af de tekniske regler, der er nødvendige for indlæsning og viderebehandling af de oplysninger, der er omhandlet i denne artikels stk. 3. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

5. De oplysninger, der er omhandlet i stk. 3, slettes samtidig med den tilsvarende indberetning eller tidligere, hvis den pågældende person anmoder herom.

6. Kun de myndigheder, der har adgangsret til den tilsvarende indberetning, må tilgå de oplysninger, der er omhandlet i stk. 3. De må udelukkende tilgå dem med henblik på at undgå fejlidentifikation.

Artikel 48

Sammenkobling af indberetninger

1. En medlemsstat kan sammenkoble indberetninger, den indlæser i SIS. Formålet hermed er at skabe en forbindelse mellem to eller flere indberetninger.

2. Sammenkoblingen påvirker ikke den særlige handling, der skal foretages på grundlag af hver enkelt sammenkoblet indberetning, eller undersøgelsesfristen for hver af de sammenkoblede indberetninger.

3. Sammenkoblingen påvirker ikke de adgangsrettigheder, som er fastsat i denne forordning. De myndigheder, der ikke har adgangsret til bestemte kategorier af indberetninger, må ikke kunne se sammenkoblingen til en indberetning, som de ikke har adgang til.

4. En medlemsstat sammenkobler indberetninger, når der er et operationelt behov herfor.

5. Når en medlemsstat finder, at det er i strid med dens nationale ret eller dens internationale forpligtelser, at en anden medlemsstat sammenkobler indberetninger, kan den træffe de nødvendige foranstaltninger for at sikre, at der ikke er adgang til de sammenkoblede indberetninger fra dens nationale område eller for de af dens myndigheder, der er etableret uden for dens område.

6. Kommissionen vedtager gennemførelsesretsakter med henblik på fastsættelse og udarbejdelse af tekniske regler for sammenkobling af indberetninger. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

Artikel 49

Formålet med de supplerende oplysninger og opbevaringsfristen herfor

1. Medlemsstaterne opbevarer en henvisning til de afgørelser, der giver anledning til en indberetning, på SIRENE-kontoret for at støtte udvekslingen af supplerende oplysninger.

2. Personoplysninger, som SIRENE-kontoret opbevarer i filer som følge af en udveksling af oplysninger, opbevares kun, så længe det er nødvendigt af hensyn til det formål, hvortil de blev givet. De skal under alle omstændigheder slettes senest et år efter, at den pågældende indberetning er blevet slettet i SIS.

3. Stk. 2 berører ikke en medlemsstats ret til i nationale filer at opbevare oplysninger om en bestemt indberetning, som den pågældende medlemsstat har indlæst, eller om en indberetning, i forbindelse med hvilken der er foretaget handlinger på dens område. Fristen for, hvor længe sådanne oplysninger må opbevares i disse filer, er undergivet national ret.

Artikel 50

Overførsel af personoplysninger til tredjeparter

Oplysninger behandlet i SIS og de tilknyttede supplerende oplysninger, som er udvekslet i henhold til denne forordning, må ikke overføres eller stilles til rådighed for tredjelande eller internationale organisationer.

Kapitel IX
Databeskyttelse

Artikel 51

Gældende lovgivning

1. Forordning (EU) 2018/…[+] finder anvendelse på eu-LISA's og Det Europæiske Agentur for Grænse- og Kystbevogtnings behandling af personoplysninger i henhold til nærværende forordning. Forordning (EU) 2016/794 finder anvendelse på Europols behandling af personoplysninger i henhold til nærværende forordning.

2. Forordning (EU) 2016/679 finder anvendelse på de i nærværende forordnings artikel 34 omhandlede kompetente myndigheders behandling af personoplysninger i henhold til nærværende forordning med undtagelse af behandling med henblik på at forebygge, afsløre, efterforske eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed, hvor direktiv (EU) 2016/680 finder anvendelse.

[+] EUT: Indsæt venligst nummeret på forordningen i PE-CONS 31/18.

Artikel 52

Ret til oplysninger

1. Tredjelandsstatsborgere, som er genstand for en indberetning i SIS, oplyses herom i henhold til artikel 13 og 14 i forordning (EU) 2016/679 eller artikel 12 og 13 i direktiv (EU) 2016/680. Disse oplysninger gives skriftligt sammen med en kopi af eller en henvisning til den nationale afgørelse, der ligger til grund for indberetningen, som omhandlet i nærværende forordnings artikel 24, stk. 1.

2. Der oplyses dog ikke herom, hvis national ret tillader en begrænsning i retten til oplysninger, navnlig for at beskytte den nationale sikkerhed, forsvaret eller den offentlige sikkerhed og forebyggelse, afsløring, efterforskning og retsforfølgning af strafbare handlinger.

Artikel 53

Ret til adgang, berigtigelse af ukorrekte oplysninger og sletning af ulovligt lagrede oplysninger

1. Registrerede skal have mulighed for at udøve deres rettigheder som anført i artikel 15, 16 og 17 i forordning (EU) 2016/679 samt artikel 14 og artikel 16, stk. 1 og 2, i direktiv (EU) 2016/680.

2. En anden medlemsstat end den indberettende medlemsstat må kun give den registrerede oplysninger om alle de af den registreredes personoplysninger, der behandles, hvis den forinden har givet den indberettende medlemsstat lejlighed til at udtale sig herom. Kommunikationen mellem disse medlemsstater sker via udveksling af supplerende oplysninger.

3. En medlemsstat træffer i overensstemmelse med national ret beslutning om helt eller delvist at undlade at give oplysninger til den registrerede, i det omfang og så længe denne undladelse er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund under behørig hensyntagen til den pågældende registreredes grundlæggende rettigheder og legitime interesser, for at:

   a) undgå, at der lægges hindringer i vejen for officielle eller retlige undersøgelser, efterforskninger eller procedurer

   b) undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner

   c) beskytte den offentlige sikkerhed

   d) beskytte den nationale sikkerhed, eller

   e) beskytte andres rettigheder og frihedsrettigheder.

I de i første afsnit omhandlede tilfælde oplyser medlemsstaten skriftligt og uden unødig forsinkelse den registrerede om enhver nægtelse eller begrænsning af adgang og om begrundelserne for nægtelsen eller begrænsningen. Disse oplysninger kan udelades, hvis udleveringen heraf vil være til skade for et af formålene i første afsnits litra a)-e). Medlemsstaten oplyser den registrerede om muligheden for at indgive klage til en tilsynsmyndighed eller at anvende retsmidler.

Medlemsstaten dokumenterer de faktiske eller retlige begrundelser for afgørelsen om ikke at udlevere oplysninger til den registrerede. Disse oplysninger stilles til rådighed for tilsynsmyndighederne.

I sådanne tilfælde kan den registrerede også udøve sine rettigheder gennem de kompetente tilsynsmyndigheder.

4. Efter en ansøgning om adgang, berigtigelse eller sletning oplyser medlemsstaten den registrerede hurtigst muligt og under alle omstændigheder inden for de frister, der er omhandlet i artikel 12, stk. 3, i forordning (EU) 2016/679, om opfølgningen på udøvelsen af rettighederne i medfør af nærværende artikel, uanset om den registrerede befinder sig i et tredjeland eller ej.

Artikel 54

Retsmidler

1. Med forbehold af bestemmelserne om retsmidler i forordning (EU) 2016/679 og direktiv (EU) 2016/680 kan enhver person indbringe et spørgsmål for enhver kompetent myndighed, herunder en domstol, i henhold til retten i enhver medlemsstat med påstand om adgang til, berigtigelse eller sletning af oplysninger, aktindsigt eller skadeserstatning i forbindelse med en indberetning vedrørende den pågældende.

2. Medlemsstaterne forpligter sig gensidigt til at fuldbyrde endelige afgørelser, der er truffet af de domstole eller myndigheder, som er omhandlet i denne artikels stk. 1, jf. dog artikel 58.

3. Medlemsstaterne rapporterer hvert år til Det Europæiske Databeskyttelsesråd om:

   a) antallet af anmodninger til den dataansvarlige om adgang og antallet af tilfælde, hvor der blev givet adgang til oplysninger

   b) antallet af anmodninger til tilsynsmyndigheden om adgang og antallet af tilfælde, hvor der blev givet adgang til oplysninger

   c) antallet af anmodninger til den dataansvarlige om berigtigelse af ukorrekte oplysninger og sletning af ulovligt lagrede oplysninger og antallet af tilfælde, hvor oplysninger blev berigtiget eller slettet

d) antallet af anmodninger til tilsynsmyndigheden om berigtigelse af ukorrekte oplysninger og sletning af ulovligt lagrede oplysninger

e) antallet af anlagte retssager

f) antallet af sager, hvor domstolen gav ansøgeren medhold

g) eventuelle bemærkninger om tilfælde af gensidig anerkendelse af endelige afgørelser truffet af domstole eller myndigheder i andre medlemsstater om indberetninger indlæst af den indberettende medlemsstat.

Kommissionen udarbejder en model for rapportering i henhold til dette stykke.

4. Rapporterne fra medlemsstaterne indarbejdes i den i artikel 57, stk. 4, omhandlede fælles rapport.

Artikel 55

Tilsyn med N.SIS

1. Medlemsstaterne sikrer, at de uafhængige tilsynsmyndigheder, der er udpeget i hver medlemsstat og har de beføjelser, der er omhandlet i kapitel VI i forordning (EU) 2016/679 eller kapitel VI i direktiv (EU) 2016/680, overvåger lovligheden af behandlingen af personoplysninger i SIS på deres område, videregivelsen heraf fra deres område og udvekslingen og viderebehandlingen af supplerende oplysninger på deres område.

2. Tilsynsmyndighederne sikrer, at der foretages en audit af databehandlingsaktiviteterne i N.SIS i overensstemmelse med internationale standarder for audit mindst hvert fjerde år. Denne audit foretages af tilsynsmyndighederne, eller tilsynsmyndighederne bestiller den direkte hos en uafhængig auditor med ekspertise inden for databeskyttelse. Tilsynsmyndighederne bevarer til enhver tid kontrollen over og påtager sig ansvaret for den uafhængige auditor.

3. Medlemsstaterne sikrer, at deres tilsynsmyndigheder har tilstrækkelige ressourcer til at udføre de opgaver, som er tillagt dem i henhold til denne forordning, og at de har adgang til rådgivning fra personer med tilstrækkeligt kendskab til biometriske data.

Artikel 56

Tilsyn med eu-LISA

1. Den Europæiske Tilsynsførende for Databeskyttelse er ansvarlig for overvågning af eu-LISA's behandling af personoplysninger og for at sikre, at behandlingen sker i overensstemmelse med denne forordning. De opgaver og beføjelser, der er omhandlet i artikel 57 og 58 i forordning (EU) 2018/…[+], finder tilsvarende anvendelse.

2. Den Europæiske Tilsynsførende for Databeskyttelse foretager mindst hvert fjerde år en audit af eu-LISA's behandling af personoplysninger i henhold til internationale standarder for audit. Der sendes en rapport om denne audit til Europa-Parlamentet, Rådet, eu-LISA, Kommissionen og tilsynsmyndighederne. eu-LISA skal have mulighed for at fremsætte bemærkninger, inden rapporten vedtages.

Artikel 57

Samarbejde mellem tilsynsmyndighederne
og Den Europæiske Tilsynsførende for Databeskyttelse

1. Tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse, der hver især handler inden for deres respektive beføjelser, samarbejder aktivt inden for rammerne af deres ansvarsområder og sikrer samordnet tilsyn med SIS.

[+] EUT: Indsæt venligst nummeret på forordningen i PE-CONS 31/18.

2. Tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse udveksler inden for deres respektive beføjelser relevante oplysninger, bistår hinanden med at gennemføre audit og inspektioner, undersøger vanskeligheder med fortolkningen eller anvendelsen af denne forordning og andre gældende EU-retsakter, undersøger problemer, som afdækkes i forbindelse med udøvelsen af uafhængigt tilsyn eller udøvelsen af den registreredes rettigheder, udarbejder harmoniserede forslag til fælles løsninger på problemer og fremmer kendskabet til databeskyttelsesrettigheder, når det er nødvendigt.

3. Til de i stk. 2 fastsatte formål mødes tilsynsmyndighederne og Den Europæiske Tilsynsførende for Databeskyttelse mindst to gange om året inden for rammerne af Det Europæiske Databeskyttelsesråd. Det Europæiske Databeskyttelsesråd dækker udgifterne til disse møder og varetager støttefunktionerne. Forretningsordenen vedtages på det første møde. Øvrige arbejdsmetoder udvikles i fællesskab efter behov.

4. Det Europæiske Databeskyttelsesråd sender hvert år Europa-Parlamentet, Rådet og Kommissionen en fælles aktivitetsrapport om det koordinerede tilsyn.

Kapitel X

Erstatningsansvar og sanktioner

Artikel 58

Erstatningsansvar

1. Med forbehold af retten til erstatning og ethvert erstatningsansvar i henhold til forordning (EU) 2016/679, direktiv (EU) 2016/680 og forordning (EU) 2018/…[+]:

   a) har enhver person eller medlemsstat, der har lidt materiel eller immateriel skade som følge af en ulovlig behandling af personoplysninger i forbindelse med brugen af N.SIS eller enhver anden handling fra en medlemsstats side, der er i strid med nærværende forordning, ret til erstatning fra nævnte medlemsstat, og

   b) har enhver person eller medlemsstat, der har lidt materiel eller immateriel skade som følge af enhver handling fra eu-LISA's side, der er i strid med nærværende forordning, ret til erstatning fra eu-LISA.

   En medlemsstat eller eu-LISA fritages helt eller delvis for deres erstatningsansvar i medfør af første afsnit, hvis de beviser, at de ikke er skyld i den begivenhed, der forårsagede skaden.

[+] EUT: Indsæt venligst nummeret på forordningen i PE-CONS 31/18.

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

3. Krav om erstatning mod en medlemsstat for den i stk. 1 og 2 omhandlede skade er underlagt den nævnte medlemsstats nationale ret. Krav om erstatning mod eu-LISA for den i stk. 1 og 2 omhandlede skade er omfattet af de betingelser, der er fastsat i traktaterne.

Artikel 59

Sanktioner

Medlemsstaterne sikrer, at misbrug af SIS-oplysninger eller behandling af sådanne oplysninger eller udveksling af supplerende oplysninger i strid med denne forordning straffes i overensstemmelse med national ret.

Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Kapitel XI
Afsluttende bestemmelser

Artikel 60

Overvågning og statistikker

1. eu-LISA sørger for, at der indføres procedurer til kontrol af, hvordan SIS fungerer set i forhold til de mål, der er fastlagt for resultater, omkostningseffektivitet, sikkerhed og tjenestens kvalitet.

2. Med henblik på den tekniske vedligeholdelse, rapportering, datakvalitetsrapportering og statistik har eu-LISA adgang til de nødvendige oplysninger vedrørende behandlingsaktiviteterne i det centrale SIS.

3. eu-LISA udarbejder daglige, månedlige og årlige statistikker over antallet af registreringer pr. indberetningskategori både for hver medlemsstat og i alt. eu-LISA forelægger også årlige rapporter over antal hit pr. indberetningskategori, antal søgninger i SIS og antal gange, hvor SIS blev brugt til at indlæse, ajourføre eller slette en indberetning, både for hver medlemsstat og i alt. Sådanne statistikker indeholder statistikker om udveksling af oplysninger i medfør af artikel 27-31. Disse statistikker må ikke indeholde personoplysninger. Den årlige statistiske rapport offentliggøres.

4. Medlemsstaterne, Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning forelægger eu-LISA og Kommissionen de oplysninger, der er nødvendige for at udarbejde de i stk. 3, 5, 7 og 8 omhandlede rapporter.

5. eu-LISA forelægger Europa-Parlamentet, Rådet, medlemsstaterne, Kommissionen, Europol, Det Europæiske Agentur for Grænse- og Kystbevogtning og Den Europæiske Tilsynsførende for Databeskyttelse de statistiske rapporter, som det udarbejder.

For at kunne overvåge gennemførelsen af EU-retsakter, herunder med henblik på forordning (EU) nr. 1053/2013, kan Kommissionen anmode eu-LISA om enten regelmæssigt eller på ad hoc-basis at forelægge yderligere specifikke statistiske rapporter om effektiviteten af SIS, brugen af SIS og udvekslingen af supplerende oplysninger.

Det Europæiske Agentur for Grænse- og Kystbevogtning kan anmode eu-LISA om at forelægge yderligere specifikke statistiske rapporter med henblik på at foretage risikoanalyser og sårbarhedsvurderinger som omhandlet i artikel 11 og 13 i forordning (EU) 2016/1624, enten regelmæssigt eller på ad hoc-basis.

6. Med henblik på artikel 15, stk. 4, og nærværende artikels stk. 3, 4 og 5, opretter, gennemfører og hoster eu-LISA et centralt register i dets tekniske anlæg, som skal indeholde de oplysninger, der er omhandlet i artikel 15, stk. 4, og nærværende artikels stk. 3, og som ikke må muliggøre identifikation af enkeltpersoner, og som skal gøre det muligt for Kommissionen og de i nærværende artikels stk. 5 omhandlede agenturer at få skræddersyede rapporter og statistikker. eu-LISA giver på anmodning og i det omfang, det er nødvendigt for varetagelsen af deres opgaver, medlemsstaterne, Kommissionen, Europol og Det Europæiske Agentur for Grænse- og Kystbevogtning sikret adgang til det centrale register via kommunikationsinfrastrukturen. eu-LISA implementerer adgangskontrol og særlige brugerprofiler for at sikre, at det centrale register udelukkende tilgås med henblik på rapportering og statistikker.

7. To år efter denne forordnings anvendelsesdato i henhold til artikel 66, stk. 5, første afsnit, og derefter hvert andet år forelægger eu-LISA Europa-Parlamentet og Rådet en rapport om det centrale SIS' og kommunikationsinfrastrukturens tekniske funktion, herunder deres sikkerhed, om AFIS og om den bilaterale og multilaterale udveksling af supplerende oplysninger mellem medlemsstaterne. Denne rapport skal desuden, når teknologien er i brug, indeholde en evaluering af anvendelsen af ansigtsbilleder til at identificere personer.

8. Tre år efter denne forordnings anvendelsesdato i henhold til artikel 66, stk. 5, første afsnit, og derefter hvert fjerde år, foretager Kommissionen en samlet evaluering af det centrale SIS og den bilaterale og multilaterale udveksling af supplerende oplysninger mellem medlemsstaterne. Denne samlede evaluering skal omfatte en vurdering af de opnåede resultater set i forhold til målene og en vurdering af, om de tilgrundliggende principper fortsat er gyldige, anvendelsen af denne forordning for så vidt angår det centrale SIS, sikkerheden i det centrale SIS og eventuelle konsekvenser for fremtidige aktiviteter. Evalueringsrapporten skal også omfatte en vurdering af AFIS og af de SIS-oplysningskampagner, som Kommissionen foretager i henhold til artikel 19.

Evalueringsrapporten skal desuden indeholde statistikker over antallet af indberetninger indlæst i henhold til artikel 24, stk. 1, litra a), og statistikker over antallet af indberetninger indlæst i henhold til nævnte stykkes litra b). Med hensyn til indberetninger, der er omfattet af artikel 24, stk. 1, litra a), skal det præciseres, hvor mange indberetninger der blev indlæst efter de situationer, som er omhandlet i artikel 24, stk. 2, litra a), b) eller c). Evalueringsrapporten skal endvidere indeholde en vurdering af medlemsstaternes anvendelse af artikel 24.

Kommissionen sender evalueringsrapporten til Europa-Parlamentet og Rådet.

9. Kommissionen vedtager gennemførelsesretsakter med henblik på fastsættelse og udarbejdelse af detaljerede regler for driften af det centrale register, der er omhandlet i denne artikels stk. 6, og de databeskyttelses- og sikkerhedsregler, der gælder for dette register. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 62, stk. 2.

Artikel 61

Udøvelse af de delegerede beføjelser

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

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 33, stk. 4, tillægges Kommissionen for en ubegrænset periode fra den … [datoen for denne forordnings ikrafttræden].

3. Den i artikel 33, stk. 4, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

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

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

6. En delegeret retsakt vedtaget i henhold til artikel 33, stk. 4, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 62

Udvalgsprocedure

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

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

Artikel 63

Ændring af forordning (EF) nr. 1987/2006

I forordning (EF) nr. 1987/2006 foretages følgende ændringer:

1) Artikel 6 affattes således:

"*Artikel 6*
Nationale systemer

1. Hver medlemsstat er ansvarlig for at oprette, drive, vedligeholde og videreudvikle sit N.SIS II og for at forbinde det med NI-SIS.

2. Hver medlemsstat er ansvarlig for at sikre uafbrudt tilgængelighed af SIS II-oplysninger for slutbrugere."

2) Artikel 11 affattes således:

"*Artikel 11*
Fortrolighed - medlemsstater

1. Hver medlemsstat anvender i overensstemmelse med national lovgivning sine egne regler for tavshedspligt eller tilsvarende fortrolighedskrav i forbindelse med alle personer og organer, der skal arbejde med SIS II-oplysninger og supplerende oplysninger. Denne pligt fortsætter med at bestå, efter at de pågældende personer er fratrådt deres stilling, eller det pågældende organs virksomhed er ophørt.

2. Hvis en medlemsstat samarbejder med eksterne kontrahenter i forbindelse med SIS II-relaterede opgaver, overvåger den nøje kontrahentens aktiviteter for at sikre overholdelsen af alle bestemmelser i denne forordning, navnlig med hensyn til sikkerhed, fortrolighed og databeskyttelse.

3. Den operationelle forvaltning af N.SIS II eller af tekniske kopier må ikke overdrages til private virksomheder eller private organisationer."

3) I artikel 15 foretages følgende ændringer:

a) følgende stykke indsættes:

"3a. Forvaltningsmyndigheden udvikler og opretholder en mekanisme og en række procedurer til udførelsen af kvalitetskontrol af oplysningerne i CS-SIS. Den forelægger regelmæssigt medlemsstaterne rapporter i forbindelse hermed.

Forvaltningsmyndigheden forelægger regelmæssigt Kommissionen en rapport vedrørende de konstaterede problemer og de berørte medlemsstater.

Kommissionen forelægger regelmæssigt Europa-Parlamentet og Rådet en rapport vedrørende konstaterede datakvalitetsproblemer."

b) stk. 8 affattes således:

"8. Den operationelle forvaltning af den centrale SIS II omfatter alle de opgaver, der er nødvendige for, at den centrale SIS II kan fungere døgnet rundt alle ugens dage i overensstemmelse med denne forordning, navnlig den vedligeholdelse og den tekniske udvikling, der er nødvendig for, at systemet kan fungere gnidningsløst. Disse opgaver omfatter også koordinering og styring af samt støtte til testaktiviteter for den centrale SIS II og N.SIS II, der sikrer, at den centrale SIS II og N.SIS II fungerer i overensstemmelse med kravene til teknisk overensstemmelse, der er fastsat i artikel 9."

4) I artikel 17 tilføjes følgende stykke:

"3. Hvis forvaltningsmyndigheden samarbejder med eksterne kontrahenter i forbindelse med SIS II-relaterede opgaver, skal den nøje overvåge kontrahentens aktiviteter for at sikre overholdelsen af alle bestemmelser i denne forordning, navnlig om sikkerhed, fortrolighed og databeskyttelse.

4. Den operationelle forvaltning af CS-SIS må ikke overdrages til private virksomheder eller private organisationer."

5) I artikel 20, stk. 2, indsættes følgende litra:

"ka) lovovertrædelsens art".

6) I artikel 21 tilføjes følgende stykke:

"Hvis afgørelsen om nægtelse af indrejse og ophold som omhandlet i artikel 24, stk. 2, er knyttet til en terrorhandling, anses sagen for at være egnet, relevant og vigtig nok til at retfærdiggøre en indberetning i SIS II. Af hensyn til den offentlige eller nationale sikkerhed kan medlemsstaterne undtagelsesvis undlade at indlæse en indberetning, når det er sandsynligt, at den kan hindre officielle eller retlige undersøgelser, efterforskninger eller procedurer."

7) Artikel 22 affattes således:

"*Artikel 22*
Særlige regler for indlæsning eller kontrol af eller søgning med fotografier og fingeraftryk

1. Fotografier og fingeraftryk må kun indlæses efter en særlig kvalitetskontrol med henblik på at vurdere, hvorvidt de lever op til minimumsstandarder for datakvalitet. Specifikationen for den særlige kvalitetskontrol fastsættes efter proceduren i artikel 51, stk. 2.

2. Når en indberetning i SIS II indeholder fotografier og fingeraftryksoplysninger, anvendes sådanne fotografier og fingeraftryksoplysninger til at bekræfte identiteten på en person, der er lokaliseret som følge af en alfanumerisk søgning i SIS II.

3. Der kan i alle tilfælde søges på fingeraftryksoplysninger for at identificere en person. Der skal dog søges på fingeraftryksoplysninger for at identificere en person, hvis en persons identitet ikke kan fastslås på anden måde. Med henblik herpå skal den centrale SIS II omfatte et automatisk fingeraftryksidentifikationssystem (AFIS).

4. Der kan også søges på fingeraftryksoplysninger i SIS II i forbindelse med indberetninger, der er indlæst i medfør af artikel 24 og 26, ved anvendelse af fuldstændige eller ufuldstændige sæt af fingeraftryk, der er fundet på et gerningssted for grov kriminalitet eller under efterforskning af terrorhandlinger, hvor det med en høj grad af sandsynlighed kan fastslås, at disse sæt af aftryk tilhører en gerningsmand, og såfremt søgningen foretages samtidigt i medlemsstatens relevante nationale fingeraftryksdatabaser."

8) Artikel 26 affattes således:

"*Artikel 26*
Betingelser for at indlæse indberetninger om tredjelandsstatsborgere, som er omfattet af restriktive foranstaltninger

1. Indberetninger om tredjelandsstatsborgere, som er omfattet af restriktive foranstaltninger, der skal forhindre indrejse i eller transit gennem medlemsstaternes område, og som er truffet i overensstemmelse med retsakter, der er vedtaget af Rådet, herunder foranstaltninger til gennemførelse af et rejseforbud udstedt af De Forenede Nationers Sikkerhedsråd, indlæses i SIS II i det omfang, at datakvalitetskravene er opfyldt, med henblik på nægtelse af indrejse og ophold.

2. Indberetningerne indlæses, ajourføres og slettes af den kompetente myndighed i den medlemsstat, der har formandskabet for Rådet for Den Europæiske Union på tidspunktet for foranstaltningens vedtagelse. Hvis denne medlemsstat ikke har adgang til SIS II eller til indberetninger indlæst i overensstemmelse med denne forordning, påhviler ansvaret den medlemsstat, der har det efterfølgende formandskab, og som har adgang til SIS II, herunder adgang til indberetninger indlæst i overensstemmelse med denne forordning.

Medlemsstaterne indfører de procedurer, der er nødvendige for at indlæse, ajourføre og slette sådanne indberetninger."

9) Følgende artikler indsættes

"*Artikel 27a*
Europols adgang til oplysninger i SIS II

1. Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol), der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2016/794*, har, hvor det er nødvendigt for at opfylde dets mandat, ret til at tilgå og søge i oplysninger i SIS II. Europol kan også udveksle og anmode om yderligere supplerende oplysninger i overensstemmelse med bestemmelserne i SIRENE-håndbogen.

2. Hvis en søgning foretaget af Europol viser, at der findes en indberetning i SIS II, underretter Europol den indberettende medlemsstat via udveksling af supplerende oplysninger ved hjælp af kommunikationsinfrastrukturen og i overensstemmelse med SIRENE-håndbogens bestemmelser. Europol underretter, indtil det bliver i stand til at anvende de funktioner, der er beregnet til udveksling af supplerende oplysninger, den indberettende medlemsstat ad de kanaler, der er fastlagt i forordning (EU) 2016/794.

3. Europol må behandle de supplerende oplysninger, der er blevet fremsendt til det af medlemsstaterne, med henblik på at sammenligne dem med sine databaser og operationelle analyseprojekter for at finde sammenhænge eller andre relevante forbindelser og til strategiske, tematiske eller operationelle analyser som omhandlet i artikel 18, stk. 2, litra a), b) og c), i forordning (EU) 2016/794. Enhver behandling af supplerende oplysninger foretaget af Europol med henblik på nærværende artikel skal udføres i overensstemmelse med nævnte forordning.

4. Europols brug af oplysninger, der er tilvejebragt gennem søgning i SIS II eller gennem behandling af supplerende oplysninger, kan kun finde sted med den indberettende medlemsstats samtykke. Hvis medlemsstaten giver tilladelse til at benytte sådanne oplysninger, skal Europols behandling finde sted i overensstemmelse med forordning (EU) 2016/794. Europol må kun meddeletredjelande og eksterne organisationer sådanne oplysninger med den indberettende medlemsstats samtykke og under fuld overholdelse af EU-retten om databeskyttelse.

5. Europol:

a) må ikke tilslutte dele af SIS II eller overføre de deri indeholdte oplysninger, som det har adgang til, til et system til dataindsamling og databehandling, der forvaltes af eller i Europol, eller downloade eller på anden måde kopiere nogen del af SIS II, jf. dog stk. 4 og 6

b) sletter uanset artikel 31, stk. 1, i forordning (EU) 2016/794 supplerende oplysninger, der indeholder personoplysninger, senest et år efter, at den pågældende indberetning er blevet slettet. Som en undtagelse hertil kan Europol, hvis det har oplysninger i sine databaser eller operationelle analyseprojekter om en sag, som de supplerende oplysninger vedrører, for at kunne udføre sine opgaver undtagelsesvis fortsat lagre de supplerende oplysninger, hvis det er nødvendigt. Europol underretter den indberettende og den fuldbyrdende medlemsstat om den fortsatte lagring af sådanne supplerende oplysninger og angiver begrundelsen herfor

c) begrænser adgangen til oplysninger i SIS II, herunder supplerende oplysninger, til særligt bemyndiget Europolpersonale, der har brug for adgang til sådanne oplysninger for at kunne udføre sine opgaver

d) vedtager og anvender foranstaltninger for at garantere sikkerhed, fortrolighed og egenkontrol i overensstemmelse med artikel 10, 11 og 13

e) sikrer, at det personale, der er bemyndiget til at behandle SIS II-oplysninger, modtager relevant uddannelse og relevante oplysninger i overensstemmelse med artikel 14, og

f) tillader Den Europæiske Tilsynsførende for Databeskyttelse at overvåge og undersøge Europols virksomhed, når det udøver sin ret til at tilgå og søge i oplysninger i SIS II og udveksler og behandler supplerende oplysninger, jf. dog forordning (EU) 2016/794.

6. Europol må kun kopiere oplysninger fra SIS II til tekniske formål, hvor sådan kopiering er nødvendig for, at behørigt bemyndiget Europolpersonale kan foretage en direkte søgning. Denne forordning finder anvendelse på sådanne kopier. Den tekniske kopi må kun anvendes til lagring af SIS II-oplysninger, mens der søges i disse. Når der er søgt i oplysningerne, skal de slettes. Sådanne anvendelser betragtes ikke som ulovlig download eller kopiering af SIS II-oplysninger. Europol må ikke kopiere indberetningsoplysninger eller uddybende oplysninger fra medlemsstaterne eller CS-SIS II til andre Europolsystemer.

7. Med henblik på at kontrollere lovligheden af databehandling, udøve egenkontrol og sikre ordentlig datasikkerhed og -integritet gemmer Europol logfiler for hver adgang til og søgning i SIS II i overensstemmelse med bestemmelserne i artikel 12. Disse logfiler og denne dokumentation betragtes ikke som ulovlig download eller kopiering af en del af SIS II.

8. Medlemsstaterne underretter ved udveksling af supplerende oplysninger Europol om eventuelle hit på indberetninger i forbindelse med terrorhandlinger. Medlemsstaterne kan undtagelsesvis undlade at underrette Europol, hvis dette ville bringe igangværende efterforskninger eller en fysisk persons sikkerhed i fare eller være i strid med væsentlige sikkerhedsinteresser i den indberettende medlemsstat.

9. Stk. 8 finder anvendelse fra den dato, hvor Europol er i stand til at modtage supplerende oplysninger i overensstemmelse med stk. 1.

Artikel 27b

Adgang til oplysninger i SIS II for europæiske grænse- og kystvagthold, hold af medarbejdere, der er involveret i tilbagesendelsesrelaterede opgaver, og medlemmerne af migrationsstyringsstøtteholdene

1. I overensstemmelse med artikel 40, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) 2016/1624** har holdmedlemmerne som omhandlet i artikel 2, nr. 8) og 9), i nævnte forordning inden for deres mandat, og forudsat at de har tilladelse til at foretage kontrol i overensstemmelse med nærværende forordnings artikel 27, stk. 1, og har fået den nødvendige uddannelse i overensstemmelse med nærværende forordnings artikel 14, ret til at tilgå og søge i oplysninger i SIS II, for så vidt det er nødvendigt for udførelsen af deres opgave, og som krævet i den operative plan for en specifik operation. Adgang til oplysninger i SIS II må ikke udvides til også at omfatte andre holdmedlemmer.

2. De i stk. 1 omhandlede holdmedlemmer udøver retten til at tilgå og søge i oplysninger i SIS II, jf. stk. 1, via en teknisk grænseflade. Den teknisk grænseflade oprettes og vedligeholdes af Det Europæiske Agentur for Grænse- og Kystbevogtning og sikrer en direkte forbindelse til den centrale SIS II.

3. Hvis en søgning foretaget af et af de i denne artikels stk. 1 omhandlede holdmedlemmer viser, at der findes en indberetning i SIS II, underrettes den indberettende medlemsstat herom. I overensstemmelse med artikel 40 i forordning (EU) 2016/1624 må holdmedlemmerne kun reagere på en indberetning i SIS II i henhold til instrukserne fra, og som hovedregel under tilstedeværelse af, grænsevagter eller medarbejdere, der er involveret i tilbagesendelsesrelaterede opgaver, fra den værtsmedlemsstat, som de opererer i. Værtsmedlemsstaten kan bemyndige holdmedlemmerne til at handle på sine vegne.

4. Med henblik på at kontrollere lovligheden af databehandling, udøve egenkontrol og sikre ordentlig datasikkerhed og -integritet gemmer Det Europæiske Agentur for Grænse- og Kystbevogtning logfiler for hver adgang til og søgning i SIS II i overensstemmelse med bestemmelserne i artikel 12.

5. Det Europæiske Agentur for Grænse- og Kystbevogtning vedtager og anvender foranstaltninger for at garantere sikkerheden, fortroligheden og egenkontrollen i overensstemmelse med artikel 10, 11 og 13 og sikrer, at de i nærværende artikels stk. 1 omhandlede hold anvender disse foranstaltninger.

6. Intet i denne artikel må fortolkes som en indskrænkning af bestemmelserne i forordning (EU) 2016/1624 om databeskyttelse eller Det Europæiske Agentur for Grænse- og Kystbevogtnings ansvar for dets uautoriserede eller forkerte behandling af oplysninger.

7. Med forbehold af stk. 2 må ingen dele af SIS II tilsluttes et system til dataindsamling og databehandling, der forvaltes af de i stk. 1 omhandlede hold eller af Det Europæiske Agentur for Grænse- og Kystbevogtning, og ingen oplysninger i SIS II, som disse hold har adgang til, må overføres til et sådant system. Ingen del af SIS II må downloades eller kopieres. Logning af adgang og søgninger betragtes ikke som ulovlig download eller kopiering af SIS II-oplysninger.

8. Det Europæiske Agentur for Grænse- og Kystbevogtning tillader Den Europæiske Tilsynsførende for Databeskyttelse at overvåge og undersøge holdenes aktiviteter, jf. denne artikel, når de udøver deres ret til at tilgå og søge i oplysninger i SIS II. Dette berører ikke de yderligere bestemmelser i Europa-Parlamentets og Rådets forordning (EU) 2018/…***[+].

---

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

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

*** Europa-Parlamentets og Rådets forordning (EU) 2018/... af ... om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT ...)."

[+] EUT: Indsæt venligst nummer i teksten og publikationsreference i fodnoten på forordningen i PE-CONS 31/18.

Artikel 64

Ændring af konventionen om gennemførelse af Schengenaftalen

Artikel 25 i konventionen om gennemførelse af Schengenaftalen udgår.

Artikel 65

Ophævelse

Forordning (EF) nr. 1987/2006 ophæves fra nærværende forordnings anvendelsesdato, jf. artikel 66, stk. 5, første afsnit.

Henvisninger til den ophævede forordning gælder som henvisninger til nærværende forordning og læses efter sammenligningstabellen i bilaget.

Artikel 66

Ikrafttræden, idriftsættelse og anvendelse

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

2. Senest den … [3 år efter denne forordnings ikrafttræden] vedtager Kommissionen en afgørelse om fastsættelse af datoen for, hvornår SIS idriftsættes i henhold til denne forordning, efter kontrol af, at følgende betingelser er opfyldt:

a) de gennemførelsesretsakter, der er nødvendige for anvendelsen af denne forordning, er blevet vedtaget

b) medlemsstaterne har meddelt Kommissionen, at de har truffet de nødvendige tekniske og retlige foranstaltninger til behandling af SIS-oplysninger og udveksling af supplerende oplysninger i henhold til denne forordning, og

c) eu-LISA har meddelt Kommissionen, at alle testaktiviteter vedrørende CS-SIS og samspillet mellem CS-SIS og N.SIS er afsluttet på tilfredsstillende vis.

3. Kommissionen overvåger nøje processen med gradvis opfyldelse af de betingelser, der er fastsat i stk. 2, og underretter Europa-Parlamentet og Rådet om resultatet af den i nævnte stykke omhandlede kontrol.

4. Senest den … [et år efter denne forordnings ikrafttræden] og derefter hvert år, indtil Kommissionen har truffet den afgørelse, som er omhandlet i stk. 2, forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om status med hensyn til forberedelsen af den fuldstændige gennemførelse af denne forordning. Denne rapport skal også indeholde detaljerede oplysninger om de afholdte udgifter og oplysninger om eventuelle risici, der kan have indvirkning på de samlede omkostninger.

5. Denne forordning finder anvendelse fra den dato, der fastsættes i overensstemmelse med stk. 2.

Uanset første afsnit:

a) finder artikel 4, stk. 4, artikel 5, artikel 8, stk. 4, artikel 9, stk. 1 og 5, artikel 15, stk. 7, artikel 19, artikel 20, stk. 3 og 4, artikel 32, stk. 4, artikel 33, stk. 4, artikel 47, stk. 4, artikel 48, stk. 6, artikel 60, stk. 6 og 9, artikel 61 og 62, artikel 63, nr. 1)-6) og 8), og nærværende artikels stk. 3 og 4 anvendelse fra datoen for denne forordnings ikrafttræden

b) finder artikel 63, nr. 9), anvendelse fra den … [et år efter denne forordnings ikrafttræden]

c) finder artikel 63, nr. 7), anvendelse fra den … [to år efter denne forordnings ikrafttræden].

6. Kommissionens afgørelse, jf. stk. 2, offentliggøres i *Den Europæiske Unions Tidende*.

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

Udfærdiget i Bruxelles, den

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

BILAG

Sammenligningstabel

Forordning (EF) nr. 1987/2006	Nærværende forordning
Artikel 1	Artikel 1
Artikel 2	Artikel 2
Artikel 3	Artikel 3
Artikel 4	Artikel 4
Artikel 5	Artikel 5
Artikel 6	Artikel 6
Artikel 7	Artikel 7
Artikel 8	Artikel 8
Artikel 9	Artikel 9
Artikel 10	Artikel 10
Artikel 11	Artikel 11
Artikel 12	Artikel 12
Artikel 13	Artikel 13
Artikel 14	Artikel 14
Artikel 15	Artikel 15
Artikel 16	Artikel 16
Artikel 17	Artikel 17
Artikel 18	Artikel 18
Artikel 19	Artikel 19
Artikel 20	Artikel 20
Artikel 21	Artikel 21

Forordning (EF) nr. 1987/2006	Nærværende forordning
Artikel 22	Artikel 32 og 33
Artikel 23	Artikel 22
–	Artikel 23
Artikel 24	Artikel 24
Artikel 25	Artikel 26
Artikel 26	Artikel 25
–	Artikel 27
–	Artikel 28
–	Artikel 29
–	Artikel 30
–	Artikel 31
Artikel 27	Artikel 34
Artikel 27a	Artikel 35
Artikel 27b	Artikel 36
–	Artikel 37
Artikel 28	Artikel 38
Artikel 29	Artikel 39
Artikel 30	Artikel 40
Artikel 31	Artikel 41
Artikel 32	Artikel 42
Artikel 33	Artikel 43
Artikel 34	Artikel 44
–	Artikel 45
Artikel 35	Artikel 46

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