Rådet for
Den Europæiske Union

Bruxelles, den 5. september 2019
(OR. en)

9364/19

DAPIX 184
ENFOPOL 252
CT 53
ENFOCUSTOM 105
CRIMORG 81
SCHENGEN 23
VISA 116
SIRIS 97
COPEN 219
ASIM 62
FRONT 190
COMIX 273
JAI 529

NOTE

fra:	Generalsekretariatet for Rådet
til:	Gruppen vedrørende Udveksling af Oplysninger og Databeskyttelse (DAPIX)
Tidl. dok. nr.:	6727/18
Vedr.:	Håndbog i udveksling af retshåndhævelsesoplysninger

1. Indledning

Håndbogen i udveksling af retshåndhævelsesoplysninger har til formål at supplere håndbogen for grænseoverskridende operationer (10505/4/09 REV4). Både indholdet i og opbygningen af håndbogen og de nationale faktablade er godkendt af Gruppen vedrørende Udveksling af Oplysninger og Databeskyttelse inden for rammerne af informationsstyringsstrategien (IMS) for EU's indre sikkerhed med henblik på at støtte, strømline og lette grænseoverskridende udveksling af oplysninger.

For at øge den praktiske værdi af håndbogen vil oversættelser til alle officielle EU-sprog blive stillet til rådighed. Desuden vil håndbogen blive ajourført to gange om året, når det er nødvendigt i lyset af ny lovgivning eller praktiske erfaringer.

Den nuværende udgave tager navnlig hensyn til Europolforordningen og kontaktoplysninger. Disse kontaktoplysninger ajourføres jævnligt af medlemsstaterne og indføres i de nationale faktablade, som fra nu af udsendes som et addendum (ADD 1) til håndbogen. Dette addendum indeholder følsomme oplysninger og må ikke videregives uden at høre Generalsekretariatet for Rådet i overensstemmelse med forordning (EF) nr. 1049/2001[1]. Et nyt element er den praktiske vejledning (ADD 2), som indeholder en sammenligning af kravene til informationsudveksling via forskellige kanaler.

2. Håndbogens formål

Håndbogen er først og fremmest tænkt som et redskab for politifolk, der arbejder på området internationale forbindelser, og navnlig for operatører af enkelte kontaktpunkter (såkaldte **"SPOC"-operatører**). Den bør derfor gøres så brugervenlig og omfattende som muligt.

Håndbogen har til formål at præge og lette det **praktiske daglige samarbejde** mellem forskellige medlemsstaters myndigheder, der er involveret i udveksling af politioplysninger både på nationalt og international plan, tjene til uddannelsesformål og sikre, at der træffes afgørelser på et mere oplyst grundlag, når det gælder om at søge efter og udveksle oplysninger på tværs af grænser.

Håndbogen indeholder **et overblik over alle EU-systemer, retsgrundlag og instrumenter til udveksling af oplysninger**, der er tilgængelige for medlemsstaternes retshåndhævende myndigheder. På denne måde er brugeren fuldt ud oplyst om de tilgængelige muligheder, når vedkommende skal beslutte, hvordan der skal søges efter eller videregives oplysninger på tværs af grænser.

Sidste del af håndbogen består af de **nationale faktablade**, der angiver relevante kontaktoplysninger og oplysninger, der er tilgængelige med henblik på grænseoverskridende udveksling. Ved regelmæssigt at ajourføre disse faktablade vil medlemsstaterne opfylde de mange underretningsforpligtelser i henhold til de forskellige instrumenter. Disse nationale faktablade bør gøre det nemmere at forvalte og finde de nødvendige oplysninger.

[1] Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter. Forordningen fastsætter de generelle principper for og begrænsninger i adgangen.

Håndbogen indeholder disse nationale faktablade samt de vigtigste praktiske oplysninger om Rådets rammeafgørelse 2006/960/RIA ("den svenske rammeafgørelse" (SFD)) og erstatter de tidligere retningslinjer for den svenske rammeafgørelse (9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

3. Håndbogens indhold

Håndbogen er inddelt i tre dele, som er udarbejdet, så de kan læses hver for sig, afhængigt af læserens hensigt.

Den første del af håndbogen består af **tjeklister**, der giver et pragmatisk overblik over muligheder for udveksling af oplysninger og praktiske aspekter i denne forbindelse. Tjeklisterne hjælper med at henvise brugeren til det relevante kontaktpunkt for udveksling af oplysninger på grundlag af lister over de tilgængelige systemer og metoder inden for følgende centrale operationelle kontekster:

– forebyggelse og efterforskning af strafbare handlinger (og ulovlig indvandring)

– bekæmpelse af terrorisme

– opretholdelse af den offentlige orden og sikkerhed

Dernæst gives der i en **generel** beskrivelse en præsentation af både de nationale organer, der er involveret i udveksling af oplysninger, og instrumenterne til udveksling af oplysninger. I håndbogen henvises der til den centrale rolle, som Rådets rammeafgørelse 2006/960/RIA ("den svenske rammeafgørelse") og Rådets afgørelse 2008/615/RIA ("Prümafgørelsen") spiller i den bredere sammenhæng med udveksling af oplysninger inden for EU. Håndbogen er dog ikke begrænset til disse instrumenter.

I addendummet suppleres manualen med

a) en samling af **nationale faktablade** for hver medlemsstat, som indeholder **praktiske oplysninger om kontaktpunkter**, der er relevante for grænseoverskridende udveksling af oplysninger, og

b) kravene til informationsudveksling med henblik på de forskellige anvendte kanaler (INTERPOL/Europol/SIRENE/ forbindelsesofficerer/PCC-centrene) og mere praktisk vejledning, der er udformet på en brugervenlig måde.

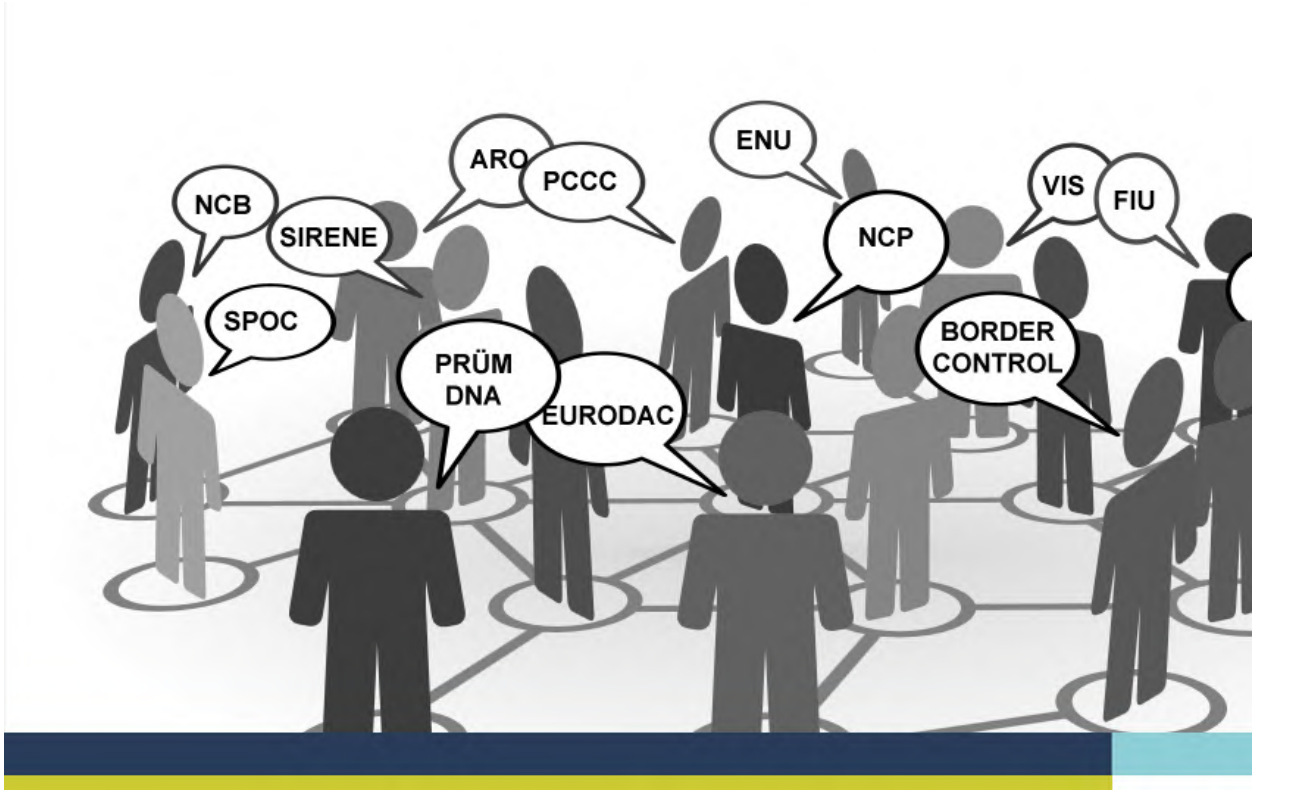
4. Det videre forløb

Udarbejdelsen af forslaget til håndbogen blev inkluderet som et tiltag i den tredje liste over tiltag i informationsstyringsstrategien, og den første udgave af håndbogen blev udarbejdet under henholdsvis det irske, cypriotiske, græske, italienske og lettiske formandskab.

Med henblik på yderligere at lette anvendelsen af håndbogen i udveksling af retshåndhævelsesoplysninger forelægger formandskabet den nuværende og ajourførte udgave for delegationerne og opfordrer dem til at formidle den på passende vis i lyset af deres behov.

Council of the European Union
General Secretariat
Directorate-General Justice and Home Affairs
Directorate Home Affairs

Manual for Law Enforcement Information Exchange



Indhold

INDLEDNING

Håndbogens formål

Grænseoverskridende politisamarbejde i Den Europæiske Union beror i høj grad på udveksling af oplysninger. Denne håndbog har til formål at lette det daglige samarbejde i denne henseende. Dens primære målgruppe er det nationale enkelte kontaktpunkt (SPOC), der er ansvarligt for at administrere strømmen af oplysninger mellem de forskellige enheder og udpegede kontaktpunkter både på nationalt og internationalt plan.

Det samlede billede af retshåndhævelsessamarbejdet[2] i Europa er karakteriset ved en stigning i og fremskyndelse af udvekslingen af oplysninger. På den ene side understøttes den af informations- og kommunikationsteknologier, der konstant udvikles. På den anden side findes der en overvældende mængde databaser både på nationalt og internationalt plan.

Denne håndbog har til formål at opfylde behovet for at identificere den relevante kontakt eller database i en specifik operationel kontekst. Den angiver i korte træk den relevante lovgivning uden dog at miste sit hovedformål, dvs. at lette grænseoverskridende udveksling af oplysninger, af syne.

Håndbogens opbygning

Håndbogen er inddelt i:

DEL I - "Operationel kontekst" **-** indeholder en række tabeller eller "tjeklister", der svarer til de oplysninger, der angives i *DEL II* og *DEL III*, inklusive enten det relevante retsgrundlag eller de relevante oplysninger om et kontaktpunkt. Disse tjeklister er inddelt i tre overordnede tematiske afsnit:

- **Forebyggelse og bekæmpelse af kriminalitet (og ulovlig indvandring) - Tjekliste A**
- **Bekæmpelse af terrorhandlinger - Tjekliste B**
- **Opretholdelse af den offentlig orden - Tjekliste C**

Formålet med disse tjeklister er at lede læseren fra det punkt, der er valgt som en passende kommunikationskanal eller -metode i en specifik operationel kontekst, hen til kilden til kontaktoplysningerne eller eventuelle relevante lovgivninger, regler og bestemmelser og håndbøger i bedste praksis.

---

[2] I denne håndbog forstås ved "retshåndhævelse" forebyggelse, afsløring eller efterforskning af terrorhandlinger som defineret i direktiv (EU) 2017/541 eller alvorlige strafbare handlinger som defineret i artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA om den europæiske arrestordre.

DEL II - "Generelle oplysninger" - angiver det samlede billede af retshåndhævelse, hvad angår de forskellige kommunikationsmetoder og -kanaler, der er tilgængelige for EU's politistyrker. Denne anden del er yderligere inddelt i tre områder, der omfatter:

- ***Kommunikationskanaler (dvs. organer, der er involveret i udvekslingen af retshåndhævelsesoplysninger)***
- ***Informationssystemer og databaser, der anvendes i grænseoverskridende udveksling af oplysninger***
- ***Lovgivning - den lovgivningsmæssige kontekst og retningslinjer vedrørende de primære kommunikationsmetoder og - systemer***

DEL III - "Nationale faktablade" i addendum 1 til denne note - indeholder nationale faktablade med detaljerede oplysninger om kontaktpunkter, der er relevante for alle aspekter af grænseoverskridende udveksling af oplysninger, der er omhandlet i hele dokumentet. Det er medlemsstaternes ansvar straks at underrette Generalsekretariatet for Rådet om eventuelle ændringer. Ved regelmæssigt at ajourføre de nationale faktablade vil medlemsstaterne opfylde de mange underretningsforpligtelser i henhold til de forskellige instrumenter. Dette bør gøre det nemmere at forvalte og finde disse oplysninger i fremtiden.

Del IV – "Praktisk vejledning for udveksling af retshåndhævelsesoplysninger"

Addendum 2 til denne note, den praktiske vejledning, indeholder på en brugervenlig måde en sammenligning af kravene til informationsudveksling med henblik på forskellige kanaler (INTERPOL/Europol/SIRENE/forbindelsesofficerer/PCC-centrene). Den indeholder desuden praktiske oplysninger og rådgivning om instrumenter til retshåndhævelsessamarbejde, som ikke kun kan være til nytte for embedsfolk ved SPOC'et, men også for andre nationale retshåndhævende myndigheder.

DEL I - Operationel kontekst

TJEKLISTE A: UDVEKSLING AF OPLYSNINGER MED HENBLIK PÅ FOREBYGGELSE OG EFTERFORSKNING AF STRAFBARE HANDLINGER

Informationssystem	**Nationalt adgangspunkt**	**Retsgrundlag**	**Håndbog**
Schengeninformationssystemet (SIS II)	SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry Bureau - anmodning om supplerende oplysninger ved det nationale grænseovergangssted)	Schengenreglerne som omhandlet i artikel 1, stk. 2, i Rådets afgørelse 1999/435/EF af 20. maj 1999 (EFT L 239 af 22.9.2000, s. 1) Rådets afgørelse 2007/533/RIA (EUT L 205 af 7.8.2007, s. 63) Forordning (EF) nr. 1986/2006 (EUT L 381 af 28.12.2006, s. 1) Forordning (EF) nr. 1987/2006 (EUT L 381 af 28.12.2006, s. 4)	Revideret udgave af det ajourførte katalog over henstillinger med henblik på korrekt anvendelse af Schengenreglerne og over bedste praksis (13039/11 SCHEVAL 126 SIRIS 79 COMIX 484) Kommissionens gennemførelsesafgørelse (EU) 2017/1528 om erstatning af bilaget til gennemførelsesafgøreles 2013/115/EU om vedtagelse af SIRENE-håndbogen og andre gennemførelsesforanstaltninger i forbindelse med anden generation af Schengeninformationssystemet (SIS II) (EUT L 231 af 7.9.2017, s. 6).

Europol/ Europols informationssystem - EIS- indekssystem Analyseregister (AWF)	National Europolenhed (ENU)	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) (gældende fra 1. maj 2017).	
INTERPOL / I-24/7	NCB (Nationalt centralbureau)	INTERPOL's regler om behandling af oplysninger (III/IRPD/GA/2011(2014)) Regler om informationskontrol og adgang til INTERPOL's akter (II.E/RCIA/GA/2004(2009))	
DNA - elektronisk søgning i udpegede nationale databaser i henhold til Prüm	Nationalt kontaktpunkt 1. trin: elektronisk søgning	Rådets afgørelse 2008/615/RIA, artikel 3 og 4 (EUT L 210 af 6.8.2008, s. 1)	
	2. trin: levering af yderligere personoplysninger og andre oplysninger	National lovgivning Rådets rammeafgørelse 2006/960/RIA (SFD) (EUT L 386 af 29.12.2006, s. 89) Berigtigelse (EUT L 75 af 15.3.2007, s. 26)	

Fingeraftryk - elektronisk søgning i et nationalt automatisk fingeraftryksidentifikationssystem (AFIS) i henhold til Prüm	Nationalt kontaktpunkt 1. trin: elektronisk søgning	Rådets afgørelse 2008/615/RIA, artikel 9 (EUT L 210 af 6.8.2008, s. 1)	
	2. trin: levering af yderligere personoplysninger og andre oplysninger	National lovgivning Rådets rammeafgørelse 2006/960/RIA (SFD)	
Oplysninger i køretøjsregistre (VRD) / Elektronisk søgning af oplysninger i køretøjsregistre i henhold til Prüm	Nationalt kontaktpunkt for indkommende anmodninger	Rådets afgørelse 2008/615/RIA, artikel 12 (EUT L 210 af 6.8.2008, s. 1)	
	for udgående anmodninger	Som ovenfor	
Passagerlisteoplysninger (PNR-oplysninger)	Passageroplysningsenhed (PIU)	Europa-Parlamentets og Rådets direktiv (EU) af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (EUT L 119 af 4.5.2016, s. 132)	

Visuminformationssystemet / VIS	Nationale centrale adgangspunkter	Rådets beslutning 2004/512/EF (EUT L 213 af 15.6.2004, s. 5) Rådets afgørelse 2008/633/RIA (EUT L 218 af 13.8.2008, s. 126) Forordning (EF) nr. 767/2008 *(EUT L 218 af 13.8.2008)* Liste over kompetente myndigheder, hvis behørigt bemyndigede medarbejdere har adgang til at indlæse, ændre, slette eller søge oplysninger i visuminformationssystemet (VIS) (EUT C 187 af 26.5.2016, s. 4)	

Eurodac	Nationale kompetente myndigheder	Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 af 26. juni 2013 om oprettelse af "Eurodac" til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet i en af medlemsstaterne af en tredjelandsstatsborger eller en statsløs og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse og om ændring af forordning (EU) nr. 1077/2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store IT-systemer inden for området med frihed, sikkerhed og retfærdighed (omarbejdning) (EUT L 180 af 29.6.2013, s. 1) *Europa-Parlamentets og Rådets forordning (EU) nr. 604/2013 af 26. juni 2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelandsstatsborger eller en statsløs i en af medlemsstaterne* (EUT L 180 af 29.6.2013, s. 31)	

Toldinformationssystemet (CIS)	Nationale adgangspunkter	Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet (EUT L 323 af 10.12.2009, s. 20)	
Det europæiske informationssystem vedrørende strafferegistre (ECRIS)	National central myndighed	Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 151 af 7.6.2019, s. 143)	ECRIS - Ikkebindende håndbog for praktikere Findes i elektronisk format hos CIRCABC på https://circabc.europa.eu
Camden Assets Recovery Inter-Agency Network (CARIN)	Kontor for inddrivelse af aktiver (ARO)	Rådets afgørelse 2007/845/RIA af 6. december 2007 om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet (EUT L 332 af 18.12.2007, s. 103)	Håndbog i bedste praksis i bekæmpelsen af økonomisk kriminalitet: en samling af gode eksempler på veludviklede systemer i medlemsstaterne til bekæmpelse af økonomisk kriminalitet (9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37)

Net af finansielle efterretningsenheder (FIU.NET)	Finansielle efterretningsenheder (FIU)	Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (EUT L 141 af 5.6.2015, s. 73) FIU'er er også for nylig blevet reguleret i Europa-Parlamentets og Rådets direktiv (EU) 2019/1153 af 20. juni 2019 om regler, der letter brugen af finansielle og andre oplysninger med henblik på forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger, og om ophævelse af Rådets afgørelse 2000/642/RIA (EUT L 186 af 11.7.2019, s. 122)	Håndbog i bedste praksis i bekæmpelsen af økonomisk kriminalitet: en samling af gode eksempler på veludviklede systemer i medlemsstaterne til bekæmpelse af økonomisk kriminalitet (9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37)

TJEKLISTE B: UDVEKSLING AF OPLYSNINGER MED HENBLIK PÅ BEKÆMPELSE AF TERRORHANDLINGER

Informationssystem	**Nationalt adgangspunkt**	**Retsgrundlag**	**Håndbog**
Schengeninformationssystemet (SIS II)	SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry Bureau - anmodning om supplerende oplysninger ved det nationale grænseovergangssted)	Schengenreglerne som omhandlet i artikel 1, stk. 2, i Rådets afgørelse 1999/435/EF af 20. maj 1999 (EFT L 239 af 22.9.2000, s. 1) Rådets afgørelse 2007/533/RIA (EUT L 205 af 7.8.2007, s. 63) Forordning (EF) nr. 1986/2006 (EUT L 381 af 28.12.2006, s. 1) Forordning (EF) nr. 1987/2006 (EUT L 381 af 28.12.2006, s. 4)	Revideret udgave af det ajourførte katalog over henstillinger med henblik på korrekt anvendelse af Schengenreglerne og over bedste praksis (13039/11 SCHEVAL 126 SIRIS 79 COMIX 484) Kommissionens gennemførelsesafgørelse (EU) 2015/219 af 29. januar 2015 om erstatning af bilaget til gennemførelsesafgørelse 2013/115/EU om vedtagelse af SIRENE-håndbogen og andre gennemførelsesforanstaltninger i forbindelse med anden generation af Schengeninformationssystemet (SIS II) (meddelt under nummer C(2015) 326)

Europol/ Europols informationssystem - EIS- indekssystem Analyseregister (AWF)	National Europolenhed (ENU)	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) (gældende fra 1. maj 2017).	
INTERPOL / I-24/7	NCB (Nationalt centralbureau)	INTERPOL's regler om behandling af oplysninger (III/IRPD/GA/2011(2014)) Regler om informationskontrol og adgang til INTERPOL's akter (II.E/RCIA/GA/2004(2009))	
DNA - elektronisk søgning i udpegede nationale databaser i henhold til Prüm	Nationalt kontaktpunkt 1. trin: elektronisk søgning	Rådets afgørelse 2008/615/RIA, artikel 3 og 4 (EUT L 210 af 6.8.2008, s. 1)	
	2. trin: levering af yderligere personoplysninger og andre oplysninger	National lovgivning Rådets rammeafgørelse 2006/960/RIA (SFD) (EUT L 386 af 29.12.2006, s. 89) Berigtigelse (EUT L 75 af 15.3.2007, s. 26)	

Fingeraftryk - elektronisk søgning i et nationalt automatisk fingeraftryksidentifikationssystem (AFIS) i henhold til Prüm	Nationalt kontaktpunkt 1. trin: elektronisk søgning	Rådets afgørelse 2008/615/RIA, artikel 9 (EUT L 210 af 6.8.2008, s. 1)	
	2. trin: levering af yderligere personoplysninger og andre oplysninger	National lovgivning Rådets rammeafgørelse 2006/960/RIA (SFD)	
Oplysninger i køretøjsregistre (VRD) / Elektronisk søgning af oplysninger i køretøjsregistre i henhold til Prüm	Nationalt kontaktpunkt for indkommende anmodninger	Rådets afgørelse 2008/615/RIA, artikel 12 (EUT L 210 af 6.8.2008, s. 1)	
	for udgående anmodninger	Som ovenfor	
DNA - elektronisk søgning i udpegede nationale databaser i henhold til Prüm	Nationalt kontaktpunkt 1. trin: elektronisk søgning	Rådets afgørelse 2008/615/RIA, artikel 3 og 4 (EUT L 210 af 6.8.2008, s. 1)	*Gennemførelsesvejledning - udveksling af DNA-oplysninger* 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61
Netværk til levering i henhold til Prüm af personoplysninger og specificerede oplysninger til forebyggelse af terrorforbrydelser	Nationalt kontaktpunkt for terrorbekæmpelse i henhold til Prüm	Rådets afgørelse 2008/615/RIA, artikel 16 (EUT L 210 af 6.8.2008, s. 1)	

Passagerlisteoplysninger (PNR-oplysninger)	Passageroplysningsenhed (PIU)	Europa-Parlamentets og Rådets direktiv (EU) af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (EUT L 119 af 4.5.2016, s. 132)	
Visuminformationssystemet / VIS	Nationale centrale adgangspunkter	Rådets beslutning 2004/512/EF (EUT L 213 af 15.6.2004, s. 5) Rådets afgørelse 2008/633/RIA (EUT L 218 af 13.8.2008, s. 126) Forordning (EF) nr. 767/2008 (EUT L 218 af 13.8.2008) Liste over kompetente myndigheder, hvis behørigt bemyndigede medarbejdere har adgang til at indlæse, ændre, slette eller søge oplysninger i visuminformationssystemet (VIS) (EUT C 187 af 26.5.2016, s. 4)	

Eurodac	Nationale kompetente myndigheder	Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 af 26. juni 2013 om oprettelse af "Eurodac" til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet i en af medlemsstaterne af en tredjelandsstatsborger eller en statsløs og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse og om ændring af forordning (EU) nr. 1077/2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store IT-systemer inden for området med frihed, sikkerhed og retfærdighed (omarbejdning) (EUT L 180 af 29.6.2013, s. 1) Europa-Parlamentets og Rådets forordning (EU) nr. 604/2013 af 26. juni 2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelandsstatsborger eller en statsløs i en af medlemsstaterne (EUT L 180 af 29.6.2013, s. 31)	

Det europæiske informationssystem vedrørende strafferegistre (ECRIS)	National central myndighed	Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 151 af 7.6.2019, s. 143)	ECRIS - Ikkebindende håndbog for praktikere Findes i elektronisk format hos CIRCABC på https://circabc.europa.eu

Europæisk strafferegistersystem for tredjelandsstatsborgere og statsløse personer (ECRIS-TCN)	National central myndighed	Europa-Parlamentets og Rådets forordning (EU) 2019/816 af 17. april 2019 om oprettelse af et centralt system til bestemmelse af, hvilke medlemsstater der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer (ECRIS-TCN) for at supplere det europæiske informationssystem vedrørende strafferegistre, og om ændring af forordning (EU) 2018/1726 (EUT L 135 af 22.5.2019, s. 1) Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 151 af 7.6.2019, s. 143)	
Camden Assets Recovery Inter-Agency Network (CARIN)	Kontor for inddrivelse af aktiver (ARO)	Rådets afgørelse 2007/845/RIA af 6. december 2007 om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet (EUT L 332 af 18.12.2007, s. 103)	

Net af finansielle efterretningsenheder (FIU.NET)	Finansielle efterretningsenheder (FIU)	Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (EUT L 141 af 5.6.2015, s. 73) FIU'er er også for nylig blevet reguleret i Europa-Parlamentets og Rådets direktiv (EU) 2019/1153 af 20. juni 2019 om regler, der letter brugen af finansielle og andre oplysninger med henblik på forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger, og om ophævelse af Rådets afgørelse 2000/642/RIA (EUT L 186 af 11.7.2019, s. 122)	

TJEKLISTE C: UDVEKSLING AF OPLYSNINGER MED HENBLIK PÅ OPRETHOLDELSE AF DEN OFFENTLIGE ORDEN OG SIKKERHED

Informationssystem	**Nationalt adgangspunkt**	**Retsgrundlag**	
Netværk af permanente kontaktpunkter vedrørende den offentlige orden	Nationale kontaktpunkter	Fælles aktion 97/339/RIA af 26. maj 1997 vedtaget af Rådet på grundlag af artikel K.3 i traktaten om Den Europæiske Union vedrørende samarbejde om offentlig orden og sikkerhed, artikel 3, litra b) *(EFT L 147 af 5.6.1997, s. 1)*	
Netværk til levering i henhold til Prüm af personoplysninger og andre oplysninger end personoplysninger med henblik på forebyggelse af strafbare handlinger og opretholdelse af den offentlige orden og sikkerhed i forbindelse med store arrangementer med en grænseoverskridende dimension	Nationalt kontaktpunkt i henhold til Prüm / store arrangementer	Rådets afgørelse 2008/615/RIA, artikel 15 (EUT L 210 af 6.8.2008, s. 1) National lovgivning	

Netværk af nationale kontaktpunkter for fodboldinformation	Nationale kontaktpunkter for fodboldinformation / NFIP	Rådets afgørelse 2002/348/RIA af 25. april 2002 om sikkerhed i forbindelse med internationale fodboldkampe (EFT L 121 af 8.5.2002, s. 1) Rådets afgørelse 2007/412/RIA af 12. juni 2007 om ændring af afgørelse 2002/348/RIA om sikkerhed i forbindelse med internationale fodboldkampe (EUT L 155 af 15.6.2007, s. 76)	Rådets henstilling (2007/C 324/07) af 6. december 2007 om håndbogen for politi og sikkerhedsmyndigheder vedrørende samarbejde ved større arrangementer med en international dimension (EUT C 314 af 22.12.2007, s. 4) Rådets resolution af 3. juni 2010 vedrørende en ajourført håndbog med henstillinger for det internationale politisamarbejde og foranstaltninger med henblik på forebyggelse og bekæmpelse af vold og uroligheder i forbindelse med fodboldkampe med international dimension, som mindst en medlemsstat deltager i (EUT C 165 af 24.6.2010, s. 1)

Netværk til beskyttelse af fremtrædende personer	Nationale adgangspunkter	Rådets afgørelse 2009/796/RIA af 4. juni 2009 om ændring af afgørelse 2002/956/RIA om oprettelse af et europæisk netværk til beskyttelse af fremtrædende personer (EUT L 283 af 30.10.2009, s. 62)	Håndbog for det europæiske netværk til beskyttelse af fremtrædende personer (10478/13 ENFOPOL 173)
Politi- og toldsamarbejdscentre	PCC-centre	Bilaterale aftaler	

DEL II - GENERELLE OPLYSNINGER

1. KONTAKTKANALER[3]

1.1. Enkelte kontaktpunkter (SPOC)

Mange nationale kontaktpunkter

Medlemsstater håndterer som anmodet såvel som anmodende stat den stigende informationsstrøm på tværs af grænserne ved at forbedre effektiviteten af de operationelle strukturer og netværk - på både nationalt og europæisk plan. Mange af EU's retsinstrumenter om grænseoverskridende retshåndhævelsessamarbejde opfordrer til oprettelse af specifikke kompetente myndigheder/organer/kontorer eller nationale kontaktpunkter (NCP'er). Politiet, toldmyndighederne eller andre kompetente myndigheder, der er bemyndiget i henhold til national ret, skal udveksle oplysninger via disse udpegede nationale kontaktpunkter (NCP'er), som i en given medlemsstat kan være placeret i forskellige afdelinger af politistyrken eller endog i forskellige ministerier. For at give et overblik findes der i del III i dette dokument en liste over de specifikke nationale kontaktpunkter for udveksling af oplysninger på EU-plan på området for udveksling af oplysninger i forbindelse med retshåndhævelse, som udsendes og ajourføres regelmæssigt af Generalsekretariatet for Rådet.

Tilgængelighedsprincippet - SFD

Udveksling af oplysninger om retshåndhævelse[4] og efterretninger af tværnational relevans bør opfylde de betingelser, der følger af "tilgængelighedsprincippet", der blev indført med "den svenske rammeafgørelse" (SFD). Det vil sige:

- at en person, der er ansat inden for de retshåndhævende myndigheder i en medlemsstat, og som har behov for oplysninger for at kunne varetage sine opgaver, kan indhente dem fra en anden medlemsstat, og

- at de retshåndhævende myndigheder i den medlemsstat, der er i besiddelse af disse oplysninger, stiller dem til rådighed til det erklærede formål under hensyntagen til den igangværende efterforsknings behov i den pågældende medlemsstat, og

---

[3] Nationale organer, der er involveret i udvekslingen af retshåndhævelsesoplysninger.

[4] I denne håndbog forstås ved "retshåndhævelse" forebyggelse, afsløring eller efterforskning af terrorhandlinger som defineret i direktiv (EU) 2017/541 eller alvorlige strafbare handlinger som defineret i artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA om den europæiske arrestordre, hvis de i henhold til national ret kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år.

- at politioplysninger, når er tilgængelige i en medlemsstat, skal deles på tværs af grænserne på samme betingelser, som gælder for informationsdeling på nationalt plan, hvilket betyder, at de regler, der anvendes i forbindelse med en grænseoverskridende sag, ikke må være strengere end dem, der anvendes i forbindelse med udveksling af oplysninger på nationalt plan ("princippet om lige adgang").

Enkelt kontaktpunkt (SPOC)

Kombinationen af de strenge krav i den svenske rammeafgørelse og eksistensen af forskellige nationale strategier til håndtering af de forskellige initiativer til udveksling af oplysninger kræver en mere enkel og ensartet strategi på medlemsstatsplan for at sikre, at alle anmodninger om oplysninger mellem retshåndhævende myndigheder i EU behandles effektivt og virkningsfuldt.

Rådets konklusioner om den europæiske informationsudvekslingsmodel (EIXM)[5], som blev vedtaget i juni 2013, anerkendte potentialet i at have et enkelt kontaktpunkt for udveksling af oplysninger inden for de enkelte medlemsstater med henblik på at bidrage til at strømline processen i en stadig mere kompleks retlig og operationel kontekst.

Politikken om at foretage så megen udveksling af oplysninger som muligt gennem et enkelt kontaktpunkt er blevet gennemført af næsten alle medlemsstater, selv om forståelsen af, hvad der definerer et SPOC, synes at variere medlemsstaterne imellem. SPOC-retningslinjerne[6] viser, hvordan SPOC'er kan struktureres for at maksimere brugen af deres ressourcer, undgå overlapning og gøre samarbejdet med andre medlemsstater mere effektivt, hensigtsmæssigt og gennemsigtigt.

Medlemsstaterne bør ud fra disse retningslinjer vælge den løsning, der passer bedst til deres situation, i lyset af det fælles aftalte mål om at styrke det internationale samarbejde, og bør overveje, hvordan de på passende måde kan informere andre medlemsstater om den valgte løsning med henblik på udveksling af bedste praksis.

---

5 Rådets konklusioner efter Kommissionens meddelelse om den europæiske informationsudvekslingsmodel (EIXM) (9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146).

6 Udkast til retningslinjer for et enkelt kontaktpunkt (SPOC) med henblik på international udveksling af retshåndhævelsesoplysninger (10492/14 DAPIX 75 ENFOPOL 157 og 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1).

Ideelt set gælder der følgende for SPOC'et:

- Det har adgang til det bredeste spektrum af relevante nationale, europæiske og internationale databaser på retshåndhævelsesområdet med henblik på hurtigt at håndtere direkte udveksling af oplysninger mellem de nationale kompetente myndigheder.

- Det huser de nationale SIRENE-, Europol- og INTERPOL-enheder.

- Det huser kontaktpunktet for forbindelsesofficererne, de kontaktpunkter, der er udpeget i henhold til den svenske rammeafgørelse og "Prümafgørelserne", samt i givet fald kontaktpunktet for de regionale og bilaterale kontorer.

- Det er etableret i sikre arbejdsomgivelser og har tilstrækkeligt og passende personale, herunder tolke- og oversættelseskapacitet, til at kunne fungere døgnet rundt/alle dage. Alt personale bør så vidt muligt uddannes og udstyres/bemyndiges til at varetage alle slags opgaver inden for SPOC'et. Hvis dette ikke er muligt, bør det sikres, at alle opgaver kan varetages døgnet rundt/alle dage af embedsmænd, der har tilkaldevagt.

- Det er en multiagenturorganisation bestående af personale, der kommer fra eller tilhører forskellige tjenester og/eller ministerier, herunder kriminalpolitiet, grænsepolitiet, toldmyndighederne og de judicielle myndigheder.

Det nationale enkelte kontaktpunkts (SPOC'ets) typiske struktur

Centralenheden for operationelt politisamarbejde

Platform for udveksling af oplysninger

*SCCOPOL er en **tværministeriel** struktur bestående af 67 politibetjente, gendarmer og toldere. Retsembedsmændene på kontoret for internationalt samarbejde i straffesager (BEPI) under justitsministeriet varetager på samme adresse også en grundlæggende tjeneste til validering af franske anmodninger om udstedelse af europæiske arrestordrer og registrering i det nationale register over efterlyste personer af begæringer om anholdelse og udenlandske efterlysninger.*

*For at sikre de tre samarbejdskanaler den nødvendige **tværgående karakter** blev der i august 2004 udpeget et centralt kontaktpunkt (CCP) i SCCOPOL. Vedkommendes vigtigste funktion er at hjælpe de franske retshåndhævende myndigheder med at vælge det bedste redskab til politisamarbejde afhængigt af den igangværende efterforsknings karakter og kompleksitet. Vedkommende kontrollerer anmodningens lovlighed, foretager den første krydskontrol og sender den videre til den mest hensigtsmæssige samarbejdskanal under hensyntagen til efterforskernes anmodning. Kun anmodninger i relation til en Schengenindberetning henhører under Sirene Frankrigs enekompetence.*

*Som følge af en vellykket ressourcesammenlægning håndterer SCCOPOL **døgnet rundt** næsten **350 000 meddelelser om året** på en **enkelt sikker platform** med et begrænset personale.*

SCCOPOL's kompetence via flere kanaler gør det muligt at sikre fransk repræsentation i europæiske grupper (SIS/VIS, SIS/SIRENE, lederne af de nationale Europolenheder (ENU)) eller INTERPOL-grupper (møder blandt INTERPOL's kontaktembedsmænd, i meddelelsesgruppen) og at fremføre et relevant operationelt synspunkt for afdelingen for internationale forbindelser (DRI), der i Frankrig har ansvaret for at føre tilsyn med de styrende organer i INTERPOL og Europol.

1.2. SIRENE-kontorer

SIRENE-kontorerne er afgørende for SIS-operationer og udveksling af oplysninger. Som led i de gældende Schengenregler[7] oprettes der i hver medlemsstat permanente SIRENE-kontorer (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry [anmodning om supplerende oplysninger ved det nationale grænseovergangssted]), som er den udpegede myndighed med centralt ansvar for den nationale del af Schengeninformationssystemet (SIS II). De er kontaktpunkt for andre kontraherende parters SIRENE-kontorer og forbindelsesleddet til nationale myndigheder og agenturer. SIS II er et hit/no hit-system baseret på søgninger. Kontorerne udveksler døgnet rundt/alle dage oplysninger vedrørende SIS II-indberetninger[8], hvor en indberetning er et sæt oplysninger, der gør det muligt for myndighederne at identificere personer eller genstande med henblik på at træffe passende forholdsregler.

Supplerende oplysninger er defineret som oplysninger, der ikke lagres i SIS II, men har tilknytning til indberetninger til SIS II, og som udveksles bilateralt eller multilateralt ved hjælp af formularer:

i) for at gøre det muligt for medlemsstaterne at konsultere og informere hinanden i forbindelse med indlæsning af en indberetning

ii) når en søgning har givet et positivt resultat, således at de rette forholdsregler kan træffes

iii) når den påkrævede forholdsregel ikke kan træffes

iv) i spørgsmål vedrørende kvaliteten af SIS II-oplysningerne

v) i spørgsmål vedrørende indberetningernes kompatibilitet og prioritet

vi) i spørgsmål vedrørende retten til adgang til systemet.

---

7 Jf. konventionen om gennemførelse af Schengenaftalen (EFT L 239 af 22.9.2000, s. 19).

8 Jf. 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).

Oplysninger skal udveksles i overensstemmelse med SIRENE-håndbogen[9] og ved hjælp af kommunikationsinfrastrukturen[10]. SIS II[11]har sammenlignet med sin forgænger forbedrede funktionaliteter som for eksempel muligheden for at indlæse fingeraftryk og fotografier, nye typer genstande (stjålne fly, både, containere, betalingsmidler) såvel som muligheden for, at indberetningens indehaver kan sammenknytte forskellige indberetninger. SIS II indeholder kopier af europæiske arrestordrer, der er direkte knyttet til indberetninger om de pågældende personer.

SIRENE-kontorerne letter politisamarbejdet og kan også spille en rolle i udvekslingen af oplysninger uden for SIS II's anvendelsesområde i henhold til de bestemmelser, der tidligere var omfattet af artikel 39 og 46 i konventionen om gennemførelse af Schengenaftalen, men som er blevet erstattet af **"den svenske rammeafgørelse"**. Artikel 12, stk. 1, i "den svenske rammeafgørelse" fastsætter, at bestemmelserne i artikel 39, stk. 1, 2 og 3, og artikel 46 i konventionen om gennemførelse af Schengenaftalen erstattes af bestemmelserne i rammeafgørelsen, for så vidt de vedrører udveksling af oplysninger og efterretninger med det formål at gennemføre kriminalefterforskninger eller kriminalefterretningsoperationer i overensstemmelse med rammeafgørelsens bestemmelser.

1.3. De nationale Europolenheder (ENU)

Hver medlemsstat har en udpeget national Europolenhed (ENU), som er forbindelsesled mellem Europol og de kompetente nationale myndigheder. ENU's forbindelsesofficerer, der er udstationeret i Europol, skal sikre direkte forbindelse døgnet rundt/alle dage mellem Europols hovedkvarter i Haag og ENU'erne i de 28 medlemsstater. Europol er også vært for forbindelsesofficerer fra ti lande og organisationer uden for EU. Netværket støttes af sikre kommunikationskanaler, som stilles til rådighed af Europol.

---

9 Kommissionens gennemførelsesafgørelse af 26. februar 2013 om vedtagelse af SIRENE-håndbogen og andre gennemførelsesforanstaltninger i forbindelse med anden generation af Schengeninformationssystemet (SIS II) (meddelt under nummer C(2013) 1043) (EUT L 71 af 14.3.2013, s. 1).

10 Som følge af lukningen af Sisnets e-mailnetværk kan SIRENE-kontorerne nu anvende sTESTA's e-mailtjeneste. Anden udveksling af oplysninger kan foregå via sTESTA-nettet, SIENA eller I-24/7-kommunikationskanalerne.

11 Rapport fra Kommissionen til Europa-Parlamentet og Rådet 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 og artikel 59, stk. 3, og artikel 66, stk. 5, i afgørelse 2007/533/RIA (15810/16 SIRIS 175 COMIX 860).

Europol[12] bistår medlemsstaternes retshåndhævende myndigheder med at forebygge og bekæmpe organiseret kriminalitet, alvorlig international kriminalitet og terrorisme, der involverer to eller flere medlemsstater. Europol er med hensyn til indsamling, lagring, behandling, analyse og udveksling af oplysninger og efterretninger afhængig af oplysninger fra medlemsstaterne. Europolforordningen fastsætter de forskellige informationsopgaver og reglerne for brug af oplysninger og udveksling af oplysninger med tredjemand på grundlag af en solid databeskyttelses- og sikkerhedsordning.

1.4. INTERPOL's nationale centralbureauer (NCB)

De **nationale centralbureauer (NCB)** i de nationale politihovedkvarterer spiller en central rolle for behandlingen i INTERPOL's informationssystem af oplysninger, som gives af deres lande. De har ret til at få direkte adgang til systemet, som omfatter:

- direkte registrering, ajourføring og sletning af data i organisationens politidatabaser såvel som etablering af forbindelser mellem data
- direkte søgning i disse databaser
- anvendelse af INTERPOL's meddelelser og cirkulærer til fremsendelse af anmodninger om samarbejde og internationale indberetninger.

NCB'erne kan hurtigt søge og krydstjekke data med direkte adgang døgnet rundt/alle dage til databaser, der indeholder oplysninger om formodede terrorister, efterlyste personer, fingeraftryk, DNA-profiler, bortkomne eller stjålne rejsedokumenter, stjålne motorkøretøjer, stjålne kunstværker mv.

---

[12] 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) (gældende fra 1. maj 2017).

Så vidt muligt bør NCB'erne give de myndigheder, der i deres lande har ansvaret for kriminalefterforskning, og som er involveret i internationalt politisamarbejde, adgang til INTERPOL's informationssystem. NCB'erne styrer omfanget af den adgang, som andre autoriserede brugere i deres lande har til INTERPOL's tjenester, og kan anmode om at blive underrettet om forespørgsler foretaget i deres nationale databaser af andre lande.

1.5. Nationale kontaktpunkter i henhold til Prüm

"Prümafgørelserne"[13] åbnede op for en ny grænseoverskridende dimension af kriminalitetsbekæmpelse ved at give gensidig grænseoverskridende onlineadgang til udpegede nationale DNA-databaser, automatiske fingeraftryksidentifikationssystemer (AFIS) og databaser over køretøjsregistreringer (VRD). Med henblik på levering af data er der udpeget et specifikt nationalt kontaktpunkt (NCP) for hver type dataudveksling i hver af de deltagende medlemsstater[14]. Databeskyttelse og skræddersyede bestemmelser om datasikkerhed tager især hensyn til den særlige karakter af onlineadgang til disse databaser. Levering af personoplysninger kræver et tilstrækkeligt niveau af databeskyttelse og -sikkerhed, som gensidigt afprøves og godkendes af medlemsstaterne, før der foretages dataudveksling.

1.5.1. NCP i henhold til Prüm - DNA og fingeraftryk

Hvad angår DNA- og fingeraftryksoplysninger er den elektroniske sammenligning af biometriske referencedata baseret på et hit/no hit-system. Referencedata gør det ikke muligt at identificere den registrerede umiddelbart. I tilfælde af et hit kan NCP'et i den søgende medlemsstat derfor anmode om yderligere specifikke personoplysninger. Der skal anmodes om levering af sådanne supplerende oplysninger via procedurer for gensidig bistand, herunder de procedurer, der blev vedtaget i henhold til "den svenske rammeafgørelse", og leveringen er omfattet af den anmodede medlemsstats nationale ret, herunder bestemmelserne om retshjælp.

---

[13] Rådets afgørelse 2008/615/RIA af 23. juni 2008 om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (EUT L 210 af 6.8.2008, s. 1). Rådets afgørelse 2008/616/RIA af 23. juni 2008 om gennemførelse af afgørelse 2008/615/RIA om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (EUT L 210 af 6.8.2008, s. 12).

[14] 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

1.5.1.1. Retningslinjer vedrørende bedste praksis for fingeraftrykssøgninger

Når en anmodende medlemsstat bruger den elektroniske fingeraftrykssøgefacilitet i henhold til Prüm, skal den følge anbefalingerne i dokumentet *Good practice for consulting Member States' databases* (14885/1/08 REV 1). Dokumentet anerkender den begrænsede søgekapacitet i forbindelse med **fingeraftryksdatabaser** og anbefaler at fremme følgende praksis på operationelt plan:

- Hvorvidt der skal søges i medlemsstaternes fingeraftryksdatabaser eller ej, og i hvilken rækkefølge sådanne søgninger foretages og gentages, er efterforskningsmæssige beslutninger, der træffes fra sag til sag, og bør ikke afgøres systematisk på forhånd.

- Der bør i princippet ikke søges i andre medlemsstaters fingeraftryksdatabaser, inden der er søgt i den anmodende medlemsstats egen/egne fingeraftryksdatabase(r).

- En beslutning om at søge i en eller flere medlemsstaters databaser bør navnlig tage hensyn til:

  – sagens alvor

  – og/eller igangværende efterforskning, navnlig oplysninger, der peger i retning af en medlemsstat eller en gruppe af medlemsstater

  – og/eller specifikke efterforskningskrav.

- Generelle søgninger bør kun foretages, når god praksis i punkt 1-3 er udtømt.

Eksempler på elektronisk dataudveksling i henhold til Rådets Prümafgørelser

I 2011 blev genetisk materiale registreret i den tjekkiske nationale DNA-database under efterforskningen af et mord. Efterforskningen blev foretaget vedrørende en mistænkt, som var flygtet til udlandet. Det genetiske materiale blev indsamlet fra et cigaretskod i et askebæger i den lejlighed, hvor forbrydelsen var blevet begået. Ved at søge i den østrigske DNA-database i 2014 blev det konstateret, at den samme profil var blevet behandlet i Østrig. De to landes SPOC'er udvekslede yderligere personoplysninger gennem politisamarbejde. Derefter blev de strafferetlige myndigheder i Østrig kontaktet og bedt om at udlevere den mistænkte til Den Tjekkiske Republik til retsforfølgning via retshjælp i straffesager.

I 2005 blev der oprettet en DNA-profil i den tjekkiske nationale DNA-database under efterforskningen af et røveri. En mistænkt blev identificeret i 2014 efter en søgning i den østrigske DNA-database. Den østrigske side blev anmodet om at fremsende et foto af nyere dato og andre personoplysninger via SPOC'erne.

1.5.2. NCP i henhold til Prüm - oplysninger i køretøjsregistre (VRD)

For så vidt angår oplysninger i køretøjsregistre kan søgninger foretages med et fuldstændigt chassisnummer i en eller alle deltagende medlemsstater eller med et fuldstændigt registreringsnummer i en specifik medlemsstat. Oplysningerne vil blive udvekslet af de NCP'er, der er udpeget for både indkommende og udgående anmodninger. Medlemsstaterne giver hinanden onlineadgang til oplysninger i nationale køretøjsregistre med hensyn til

a) oplysninger vedrørende ejere eller indehavere, og

b) oplysninger vedrørende køretøjer.

Medlemsstaterne anvender en version af softwareprogrammet til det europæiske informationssystem vedrørende køretøjer og kørekort (Eucaris), som er udformet specielt med henblik på Prüm og på at foretage sådanne søgninger. Søgninger af oplysninger i køretøjsregistre adskiller sig fra DNA- og fingeraftrykssøgninger ved at give både personoplysninger og referencedata i tilfælde af et hit. Som med andre elektroniske søgninger er det underforstået, at levering af personoplysninger er betinget af, at de modtagende medlemsstater har et passende databeskyttelsesniveau.

1.5.3. NCP for forebyggelse af terrorisme i henhold til Prüm

Udpegede NCP'er kan efter anmodning eller på eget initiativ udveksle oplysninger om personer, der mistænkes for at begå terrorforbrydelser. Oplysningerne omfatter mistænktes efternavn, fornavne, fødselsdato og fødested samt en beskrivelse af de forhold, der giver anledning til formodningen om, at den registrerede vil begå strafbare handlinger forbundet med terrorvirksomhed.

Den leverende medlemsstat kan under overholdelse af national ret fastsætte betingelser for brugen af oplysningerne i den modtagende medlemsstat, som er bundet af sådanne betingelser.

1.5.4. NCP for store arrangementer i henhold til Prüm

Medlemsstater, der skal være vært for større arrangementer med en international dimension, skal garantere sikkerheden omkring arrangementet for så vidt angår både aspektet vedrørende den offentlige orden og aspektet vedrørende terrorbekæmpelse. Afhængig af arrangementets art (politisk, sportsligt, socialt, kulturelt eller andet) kan det ene aspekt være mere relevant end det andet. Begge aspekter skal imidlertid tages med i betragtning, selv om de måske hører under andre myndigheder. Der lægges særlig vægt på fænomenet med voldsudøvere, der rejser fra land til land, navnlig med hensyn til internationale fodboldkampe.

Med henblik på forebyggelse af strafbare handlinger og opretholdelse af den offentlige orden og sikkerhed i forbindelse med større arrangementer og lignende forsamlinger af store menneskemængder (af politisk, sportslig, social, kulturel eller anden art), katastrofer og alvorlige ulykker med grænseoverskridende følger kan udpegede NCP'er efter anmodning eller på eget initiativ levere hinanden

- andre oplysninger end personoplysninger, eller
- personoplysninger, hvis endelige domme eller andre forhold lader formode, at de pågældende personer vil begå strafbare handlinger under arrangementerne, eller at de udgør en fare for den offentlige orden og sikkerhed.

Personoplysningerne må kun behandles til de formål, der er anført ovenfor, og i forbindelse med de specifikke arrangementer, med henblik på hvilke de er leveret. De leverede oplysninger skal straks slettes, når disse formål er opfyldt, og under alle omstændigheder efter højst et år. Oplysningerne leveres i overensstemmelse med den leverende medlemsstats nationale ret.

1.5.4.1. Håndbog vedrørende samarbejde ved større arrangementer med en international dimension[15]

Denne håndbog indeholder retningslinjer og forslag til retshåndhævende myndigheder, hvis opgave er at garantere den offentlige sikkerhed ved større arrangementer som De Olympiske Lege eller andre større sportsbegivenheder, sociale arrangementer eller politiske møder på højt niveau.

Håndbogen, som hele tiden ændres og tilpasses udviklingen af bedste praksis, indeholder vejledning til informationsstyring og styring af arrangementer samt til evaluering i tilknytning til arrangementerne og strategisk evaluering. Standardformularerne i bilaget vedrører:

- anmodning om forbindelsesofficerer
- risikoanalyse vedrørende potentielle demonstranter og andre grupperinger
- udveksling af oplysninger om enkeltpersoner eller grupper, der udgør en terrortrussel
- en liste over referencedokumenter
- en tabel med permanente nationale kontaktpunkter vedrørende den offentlige orden.

1.6. Nationale kontaktpunkter for fodboldinformation (hos politiet) (NFIP)[16]

Foruden NCP'et for store arrangementer i henhold til Prüm og med særlig henblik på internationale fodboldkampe pålægges det et nationalt kontaktpunkt for fodboldinformation (NFIP) i hvert medlemsstat at udveksle relevante oplysninger og udforme grænseoverskridende politisamarbejde. Taktisk, strategisk og operationel information kan benyttes af selve NFIP'et eller videresendes til de relevante myndigheder eller politiet.

Kontakter mellem politiet i de forskellige lande, der er involveret i en begivenhed, koordineres og, hvis det er nødvendigt, organiseres af NFIP'et. Det CIV-baserede websted for NFIP'er (www.nfip.eu) formidler oplysninger og rådgivning om tilgængelige retlige og andre muligheder vedrørende tryghed og sikkerhed i forbindelse med fodboldkampe.

---

15 Rådets henstilling 2007/C 314/02 af 6. december 2007 om håndbogen for politi og sikkerhedsmyndigheder vedrørende samarbejde ved større arrangementer med en international dimension (EUT C 314 af 22.12.2007 s. 4).

16 Rådets afgørelse 2002/348/RIA af 25. april 2002 om sikkerhed i forbindelse med internationale fodboldkampe (EFT L 121 af 8.5.2002, s. 1).

NFIP'et koordinerer behandlingen af oplysninger om højrisikotilhængere med henblik på at forberede og træffe passende foranstaltninger til opretholdelse af den offentlige orden i forbindelse med en fodboldkamp. Dette omfatter især oplysninger om enkeltpersoner, som udgør eller kan udgøre en fare for den offentlige orden og sikkerhed. Oplysningerne bør udveksles ved hjælp af formularerne[17] i bilaget til fodboldhåndbogen.

1.6.1. Fodboldhåndbogen[18]

Fodboldhåndbogen findes som bilag til Rådets resolution 2006/C 322/01 og giver eksempler på, hvordan politiet bør samarbejde på internationalt plan for at forebygge og bekæmpe vold og uroligheder i forbindelse med fodboldkampe. Indholdet består navnlig af henstillinger vedrørende:

- politiets informationsstyring
- tilrettelæggelsen af politiets samarbejde
- en tjekliste vedrørende mediepolitik og kommunikationsstrategi (politi/myndigheder).

1.7. Politi- og toldsamarbejdscentre (PCCC)

PCCC'erne oprettes på grundlag af bi- eller multilaterale aftaler i henhold til artikel 39, stk. 4, i konventionen om gennemførelse af Schengenaftalen (SGK). De kontraherende parter fastlægger i disse aftaler grundlaget for deres grænseoverskridende samarbejde, herunder opgaverne, retsgrundlaget og procedurerne for oprettelse og drift af centrene. PCCC'erne samler personale fra nabolandene og er tæt knyttet til nationale organer, der beskæftiger sig med internationalt samarbejde (NCP'er, INTERPOL's NCB'er, ENU'er, SIRENE-kontorerne).

---

17 Rådets afgørelse 2007/412/RIA af 12. juni 2007 om ændring af afgørelse 2002/348/RIA om sikkerhed i forbindelse med internationale fodboldkampe (EUT L 155 af 15.6.2007, s. 76).

18 Rådets resolution vedrørende en ajourført håndbog med henstillinger for det internationale politisamarbejde og foranstaltninger med henblik på forebyggelse og bekæmpelse af vold og uroligheder i forbindelse med fodboldkampe med international dimension, som mindst en medlemsstat deltager i ("EU's fodboldhåndbog") (2016/C 444/01) (EUT C 444 af 29.11.2016, s. 1).

PCCC'erne yder rådgivning og ikkeoperativ støtte til det nationale operationelle politi, toldvæsenet og andre myndigheder i den grænseregion, hvor de er beliggende. PCCC'ernes personale skal hurtigt tilvejebringe de oplysninger, der anmodes om, jf. Rådets afgørelse 2006/960/RIA ("den svenske rammeafgørelse").

Ved udgangen af 2016 var 8 af de 59 eksisterende PCCC'er tilknyttet SIENA, Europols netværksprogram til sikker informationsudveksling. Udveksling af oplysninger via PCCC'erne vedrører især småkriminalitet og noget mere alvorlig kriminalitet, ulovlige migrationsstrømme og problemer med den offentlige orden. Sådanne oplysninger kan omfatte identifikation af førere af motorkøretøjer eller kontrol af relevansen eller ægtheden af identitets- og rejsedokumenter.

De kontraherende parter kan i fællesskab beslutte at omdanne et PCCC til et regionalt operativt koordinationscenter, der betjener alle berørte myndigheder, navnlig i tilfælde af regionale hændelser (naturkatastrofer) eller større arrangementer (De Olympiske Lege, VM i fodbold osv.).

Hvis et PCCC modtager oplysninger, som henhører under de nationale centrale enheder, skal disse oplysninger straks videresendes til SPOC'et/den centrale enhed. Hvis et PCCC modtager oplysninger, der åbenlyst har interesse for Europol, kan det videresende disse oplysninger til den ENU, der hører under SPOC'et, som så selv videregiver oplysningerne til Europol.

Eksempel på udveksling af oplysninger gennem et PCCC

EPICC ("Euregio Police Information and Cooperation Centre") er kortformen for PCCC'et i Heerlen.

Det blev oprettet ad hoc (intet specifikt retligt instrument) i 2005 på initiativ af "NeBeDeAgPol", der er en sammenslutning af politichefer i EU-regionen Meuse-Rhinen, der ligger i grænseområdet mellem Nederlandene, Belgien og Tyskland - et af de tættest befolkede grænseområder i Den Europæiske Union.

På dette PCCC arbejder ca. tredive belgiske, tyske og nederlandske politibetjente sammen på samme platform.

Disse betjente har adgang på stedet til det meste af indholdet af deres respektive landes databaser. På den måde kan de - på meget kort tid - levere nøjagtige, fuldstændige og pålidelige oplysninger efter anmodning fra politiet om Belgien, Tyskland eller Nederlandene. Udvekslingen af oplysninger mellem de tre EPICC-delegationer foregår gennem Europolprogrammet "SIENA".

EPICC indsamler og analyserer tilgængelige politioplysninger i grænseområdet for at påvise, beskrive og følge grænsesikkerhedsproblemer (nye fænomener eller fremgangsmåder, grupper af kriminelle, der er aktive i grænseområdet, arrangementer eller personer, der kræver særlig opmærksomhed osv.).

PCCC i Heerlen kan takket være sin særlige ekspertise og blandede sammensætning yde effektiv støtte i forbindelse med forberedelse og gennemførelse af grænseoverskridende operationer, efterforskninger eller overvågningsforanstaltninger.

1.8. Forbindelsesofficerer (LO)

Artikel 47 i konventionen om gennemførelse af Schengenaftalen (SGK) fastsætter, at medlemsstaterne *"kan indgå bilaterale aftaler om tidsbegrænset eller tidsubegrænset udstationering af forbindelsesofficerer ved en anden [medlemsstats] politi."*
Forbindelsesofficerernes rolle er at etablere og fastholde direkte kontakter for at fremme og fremskynde samarbejdet med henblik på bekæmpelse af kriminalitet, navnlig ved at yde bistand. Forbindelsesofficerer har ikke kompetence til at udføre politiopgaver på egen hånd. De sikrer hurtigt og effektivt samarbejde baseret på personlig kontakt og gensidig tillid ved:

- at facilitere og fremskynde indsamling og udveksling af oplysninger
- at bistå med efterkommelse af anmodninger om gensidig retshjælp mellem landenes politi og retsvæsen i straffesager
- at tilrettelægge og sikre grænseoverskridende operationer.

Forbindelsesofficerer kan udstationeres til andre medlemsstater, tredjelande eller EU-agenturer eller internationale organisationer. Kompendiet[19] om forbindelsesofficerer i forbindelse med retshåndhævelse, som Rådets Generalsekretariat ajourfører årligt, redegør for forbindelsesofficerernes arbejde og opgaver og indeholder fortegnelser over forbindelsesofficerer, herunder kontaktoplysninger.

På grundlag af tidligere og løbende erfaringer i de forskellige værtslande og med henblik på at opnå større sammenlægning af medlemsstaternes aktiviteter i forhold til tredjelande med hensyn til både forbindelsesofficerernes arbejde og teknisk samarbejde er der i kompendiet indkredset en række eksempler på bedste praksis. Det foreslås, at medlemsstaternes forbindelsesofficerer og deres relevante myndigheder anvender disse, når det er hensigtsmæssigt.

---

[19] "Update of the Compendium on law enforcement liaison officers (2018)" (10095/1/18 REV 1 ENFOPOL 397 JAIEX 84 COMIX 422).

Typiske eksempler på udveksling af oplysninger mellem forbindelsesofficerer

- *Forbindelsesofficerer kan få til opgave at sikre kontakt med henblik på at etablere direkte samarbejde i specifikke sager som f.eks. narkotikakriminalitet.*
- *Forbindelsesofficerer kan opgive specifikke oplysninger om nationale regler og lovgivning vedrørende internationalt politisamarbejde eller retshjælp i straffesager.*
- *Forbindelsesofficerer fører i nogle tilfælde ajourførte lister over de ansvarlige myndigheder i deres medlemsstater.*
- *Forbindelsesofficerer har også i nogle medlemsstater fået til opgave at håndtere anmodninger om samarbejde i henhold til artikel 17 i Prümafgørelsen (Fælles operationer). Den danske LO hos Europol blev f.eks. af Den Tjekkiske Republik bedt om at videresende en anmodning til Danmark om at udpege fire danske politibetjente til at hjælpe med en sag, der involverede begge medlemsstater.*

1.9. Medlemsstaternes kontorer for inddrivelse af aktiver (ARO)

Økonomisk kriminalitet omfatter en lang række aktiviteter såsom falskmøntneri, korruption og svig (f.eks. kreditkortbedrageri, svindel med realkreditlån, sundhedssystemet eller værdipapirer, bestikkelse eller underslæb, hvidvask af penge, identitetstyveri og skatteunddragelse). Der opnås forbedret samarbejde gennem tættere grænseoverskridende samarbejde mellem kontorer for inddrivelse af aktiver (ARO'er), finansielle efterretningsenheder (FIU'er) og politi- og toldmyndigheder[20].

Efter vedtagelsen af Rådets afgørelse 2007/845/RIA af 6. december 2007 om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet[21] har alle medlemsstater etableret og udpeget kontorer for inddrivelse af aktiver (ARO'er). Disse specialiserede enheder har udviklet sig til et fasttømret netværk af specialister, der direkte kan udveksle oplysninger om spørgsmål vedrørende inddrivelse af aktiver gennem SIENA-systemet. Under ledelse af Europa-Kommissionen og Europol fremmer ARO-netværket samarbejdet mellem medlemsstaternes ARO'er samt strategiske drøftelser og udveksling af bedste praksis. Europols kontor for formuegoder forbundet med kriminalitet (ECAB) fungerer som kontaktpunkt for inddrivelse af aktiver i EU.

Bestemmelserne i Europa-Parlamentets og Rådets direktiv 2014/42/EU af 3. april 2014 om indefrysning og konfiskation af redskaber og udbytte fra strafbart forhold i Den Europæiske Union[22] vil yderligere forbedre effektiviteten af samarbejdet mellem kontorerne for inddrivelse af aktiver i Den Europæiske Union. Medlemsstaterne opfordres til at gennemføre direktivet i national ret senest den 4. oktober 2016.

---

20 Håndbog i bedste praksis i bekæmpelsen af økonomisk kriminalitet: Gode eksempler på veludviklede systemer i medlemsstaterne til bekæmpelse af økonomisk kriminalitet (9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144).

21 Rådets afgørelse 2007/845/RIA af 6. december 2007 om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet (EUT L 332 af 18.12.2007, s. 103).

22 Europa-Parlamentets og Rådets direktiv 2014/42/EU af 3. april 2014 om indefrysning og konfiskation af redskaber og udbytte fra strafbart forhold i Den Europæiske Union (EUT L 127 af 29.4.2014, s. 39).

Camden Assets Recovery Inter-Agency Network (CARIN), der blev oprettet i 2004 for at støtte grænseoverskridende identifikation, indefrysning, beslaglæggelse og konfiskation af formuegoder, styrker den gensidige udveksling af oplysninger om forskellige nationale tilgange, der går ud over EU.

CARIN-netværket omfatter pr. 2015 aktører fra 53 jurisdiktionsområder og ni internationale organisationer, der fungerer som kontaktpunkter med henblik på hurtig grænseoverskridende udveksling af oplysninger efter anmodning eller spontant. Nationale ARO'er samarbejder indbyrdes eller med andre myndigheder, der faciliterer opsporing og identifikation af udbytte fra strafbart forhold. Alle medlemsstater har oprettet et ARO, men der er alligevel store forskelle mellem medlemsstaterne med hensyn til organisatorisk opbygning, ressourcer og aktiviteter.

De oplysninger, der udveksles, kan benyttes i henhold til bestemmelserne om databeskyttelse i de modtagende medlemsstater og er omfattet af de samme regler for databeskyttelse, som hvis oplysningerne var indsamlet i den modtagende medlemsstat. Uanmodet udveksling af oplysninger i henhold til denne afgørelse og under anvendelse af de procedurer og tidsfrister, der er fastsat i den svenske rammeafgørelse, skal fremmes.

1.10. Hvidvask af penge - samarbejde mellem finansielle efterretningsenheder (FIU)[23][24]

Relevante oplysninger om ethvert forhold, der kan være tegn på hvidvask af penge eller finansiering af terrorisme, bør indberettes til de nationale finansielle efterretningsenheder (FIU'er). FIU'er analyserer modtagne oplysninger fra sag til sag med det sigte at konstatere, om der er forbindelser mellem mistænkelige transaktioner og bagvedliggende kriminelle aktiviteter, for at forebygge og bekæmpe hvidvask af penge og finansiering af terrorisme. FIU'en fungerer som en central national enhed, der modtager, analyserer og formidler resultaterne af sine analyser til de kompetente myndigheder. Eftersom FIU'en er operationelt uafhængig og selvstændig, varetager den sine funktioner frit, herunder den selvstændige beslutning om at analysere, rekvirere og formidle specifikke oplysninger.

---

[23] Europa-Parlamentets og Rådets direktiv (EU) 2019/1153 af 20. juni 2019 om regler, der letter brugen af finansielle og andre oplysninger med henblik på forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger, og om ophævelse af Rådets afgørelse 2000/642/RIA (EUT L 186 af 11.7.2019, s. 122).

[24] Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (EUT L 141 af 5.6.2015, s. 73).

FIU'erne fungerer også som nationale kontaktpunkter for grænseoverskridende udveksling af oplysninger. Som med kontorerne for inddrivelse af aktiver er der stor variation mellem medlemsstaterne med hensyn til FIU'ernes organisatoriske opbygning, funktioner og ressourcer. De anbringes enten under de judicielle myndigheder eller inden for politiet, eller de oprettes som en "hybrid", der sammenlægger kompetencerne hos politiet og anklagemyndigheden. Denne forskelligartethed kan sommetider medføre hindringer for det internationale samarbejde.

Da hvidvask af penge og finansiering af terrorisme imidlertid er af tværnational karakter, er koordinering og samarbejde mellem FIU'er af allerstørste betydning. Med henblik på at forbedre koordineringen og samarbejdet og for at sikre, at indberetninger af mistænkelige transaktioner når frem til FIU'en i den medlemsstat, hvor indberetningen vil gøre størst gavn, er der fastsat detaljerede bestemmelser i direktiv (EU) 2015/849. Med det sigte hurtigt, konstruktivt og effektivt at skabe det bredest mulige grænseoverskridende samarbejde bør medlemsstaterne navnlig sikre, at deres FIU'er udveksler oplysninger frit, uopfordret eller efter anmodning med tredjelandes finansielle efterretningsenheder.

Forbedringen af udvekslingen af oplysninger mellem FIU'er i Unionen bør ske under anvendelse af sikre faciliteter, navnlig det decentraliserede computernetværk FIU.NET. Alle 28 FIU'er er koblet til FIU.NET. Det har over de seneste år udviklet sig fra et sikkert grundlæggende redskab til struktureret bilateral udveksling af oplysninger til et sikkert multifunktionelt redskab til multilateral udveksling af oplysninger med både sagsbehandlingsfunktioner og halvautomatiseret standardisering af processer. I FIU.NET er hver ny funktion og automatisk proces valgfri uden forbehold. De enkelte FIU'er kan beslutte, hvilke af FIU.NET's muligheder og funktioner de vil bruge. De anvender kun de funktioner, som de føler sig trygge ved, og undlader at bruge dem, som de ikke har brug for eller ikke vil bruge.

1.11. Napoli II-konventionen[25]

Medlemsstaterne yder hinanden bistand inden for rammerne af Napoli II-konventionen med henblik på at forebygge og efterforske overtrædelser af nationale toldbestemmelser og forfølge og straffe overtrædelser af EF-toldbestemmelser og nationale toldbestemmelser. Med hensyn til kriminalefterforskninger fastlægger konventionen procedurer, som gør det muligt for toldmyndighederne at handle i fællesskab og udveksle oplysninger uden forudgående anmodning eller efter anmodning, om ulovlig handel.

Anmodningerne fremsættes skriftligt på et officielt sprog i den bistandssøgte myndigheds medlemsstat eller på et for denne myndighed acceptabelt sprog. Standard for meddelelsen af oplysninger fastsættes i en formular. De berørte myndigheder meddeler alle oplysninger, der kan være nyttige i forbindelse med at forebygge, efterforske og forfølge overtrædelser. De udveksler personoplysninger, dvs. alle oplysninger om en identificeret eller identificerbar fysisk person.

Ved ydelse af bistand optræder den bistandssøgte myndighed eller den kompetente myndighed, som førstnævnte har indbragt sagen for, på samme måde, som hvis den handlede på egne vegne eller efter anmodning fra en anden myndighed i sit hjemland.

Håndbogen for Napoli II-konventionen om gensidig bistand og samarbejde mellem toldmyndighederne er opdelt i tre dele, som fastlægger:

- de generelle bestemmelser i 13615/05 ENFOCUSTOM 61 + COR 1 (CZ)
- de nationale emneblade som ajourført i 2016 i 15429/16 JAI 1028 ENFOCUSTOM 238
- bilagene, herunder standardformularerne for fremsendelse af oplysninger i 13615/05 ENFOCUSTOM 61 ADD 1.

[25] Rådets retsakt af 18. december 1997 om udarbejdelse, på grundlag af artikel K.3 i traktaten om Den Europæiske Union, af konventionen om gensidig bistand og samarbejde mellem toldmyndighederne (EFT C 24 af 23.1.1998, s. 1).

1.12. Passageroplysningsenhed (PIU)

Inden for rammerne af direktiv 2016/681[26] opretter eller udpeger hver medlemsstat en passageroplysningsenhed (PIU). Sådanne enheder er ansvarlige for behandling af passagerlisteoplysninger (PNR-oplysninger) fra luftfartsselskaber[27] og udgør desuden den vigtigste kanal for udveksling af oplysninger mellem medlemsstaterne og med Europol. To eller flere medlemsstater kan oprette eller udpege en enkelt myndighed til at fungere som deres fælles passageroplysningsenhed.

Behandlingen af PNR-oplysninger tjener hovedsagelig til vurdering af flypassagerer for at identificere personer, som skal undersøges nærmere af de nationale myndigheder, der har kompetence til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet. Direktivet finder anvendelse på flyvninger uden for EU og kan desuden anvendes på flyvninger inden for EU, hvis en medlemsstat beslutter at gøre det.

Vurderingen af PNR-oplysninger gør det lettere at identificere personer, som forud for denne vurdering ikke var mistænkt for at være involveret i terrorhandlinger eller grov kriminalitet. I overensstemmelse med EU's databeskyttelsespolitik skal behandlingen af disse oplysninger være både relevant og nødvendig og stå i rimeligt forhold til de specifikke sikkerhedsmål, der forfølges i dette direktiv.

---

[26] Europa-Parlamentets og Rådets direktiv (EU) 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (EUT L 119 af 4.5.2016, s. 132).

[27] Direktivet påvirker ikke medlemsstaternes mulighed for at indføre et system i national ret til indsamling og behandling af PNR-oplysninger fra erhvervsdrivende, der ikke er luftfartsselskaber, f.eks. rejsebureauer og rejsearrangører, der leverer rejserelaterede tjenester, herunder reservation af flyvninger, for hvilke de indsamler og behandler PNR-oplysninger, eller fra andre transportvirksomheder end dem, der er nævnt i direktivet, forudsat at sådan national ret er i overensstemmelse med EU-retten.

PIU'erne ansvarlige for:

- på nationalt plan at indsamle PNR-oplysninger fra luftfartsselskaber, opbevare og behandle disse data og overføre dem eller resultatet af behandlingen heraf til de nationale kompetente myndigheder

- på EU-niveau at udveksle PNR-oplysninger og resultatet af behandlingen heraf

    a) indbyrdes. I hastetilfælde og på visse betingelser kan ovennævnte nationale kompetente myndigheder dog anmode en anden medlemsstats PIU direkte om at overdrage dem PNR-oplysninger, der opbevares i sidstnævntes database, og

    b) med Europol, som er berettiget til inden for rammerne af sine kompetencer og med henblik på at udføre sine opgaver at anmode om sådanne oplysninger fra PIU'er.

PIU'er skal udelukkende varetage deres opgaver på et sikkert sted på en medlemsstats område. De PNR-oplysninger, der er sendt til PIU'er, skal lagres i en database i en periode på fem år efter videregivelsen til PIU'en i ankomst- eller afrejsemedlemsstaten. Seks måneder efter videregivelsen skal alle PNR-oplysninger imidlertid anonymiseres ved at maskere de dataelementer, der er fastsat i direktivet, og som kan tjene til at identificere den registrerede direkte. Resultatet af behandlingen skal kun opbevares af PIU'en så længe, som det er nødvendigt for at underrette de relevante kompetente nationale myndigheder og andre medlemsstaters PIU'er om et positivt match.

PIU'en behandler kun de oplysninger, der er opført i direktivets bilag I, med henblik på:

- at foretage en vurdering af passagerer forud for deres planlagte ankomst til eller afrejse fra medlemsstaten for at identificere personer, som skal undersøges nærmere af nationale myndigheder, og, hvor det er nødvendigt, af Europol

- i konkrete tilfælde efter anmodning fra de kompetente myndigheder at udlevere og behandle PNR-oplysninger i specifikke tilfælde og forelægge disse myndigheder og i givet fald Europol resultaterne af denne behandling

- at analysere PNR-oplysninger med henblik på at ajourføre eller fastsætte nye kriterier, der skal anvendes for at identificere passagerer, der kan være involveret i en terrorhandling eller grov kriminalitet.

Ved en sådan vurdering kan PIU'en enten samkøre PNR-oplysninger med oplysninger i databaser, der er relevante med henblik på at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, i overensstemmelse med gældende EU-regler og internationale og nationale regler for sådanne databaser eller behandle PNR-oplysninger efter forudbestemte relevante kriterier. Disse forudbestemte kriterier skal være målrettede, stå i rimeligt forhold til målet og være specifikke. Det er op til PIU'erne at opstille og jævnligt revidere disse kriterier i samarbejde med de relevante kompetente myndigheder. Disse kriterier må ikke baseres på følsomme personoplysninger om f.eks. race eller etnisk oprindelse, politiske anskuelser, religiøs eller filosofisk overbevisning, medlemskab af en fagforening, sundhed, seksualitet eller seksuel orientering.

Hvad angår personer, der identificeres, videresender PIU'en alle relevante og nødvendige PNR-oplysninger eller resultatet af behandlingen heraf til de tilsvarende PIU'er i de øvrige medlemsstater. Disse PIU'er videresender de modtagne oplysninger til deres egne kompetente myndigheder.

Den databeskyttelsesansvarlige udnævnes af den PIU, der er ansvarlig for at overvåge behandlingen af PNR-oplysninger. Den registrerede har ret til at kontakte den databeskyttelsesansvarlige som et enkelt kontaktpunkt om alle spørgsmål vedrørende behandlingen af den pågældende registreredes PNR-oplysninger.

Alle overførsler af PNR-oplysninger fra luftfartsselskaber til PIU'er skal foretages ad elektronisk vej, der garanterer den tekniske sikkerhed. Med henblik herpå er både de fælles protokoller, som luftfartsselskaberne skal overholde ved overførsel af oplysninger, og de understøttede dataformater, der sikrer læsbarheden af oplysningerne for alle relevante parter, fastlagt på EU-plan[28].

[28] Kommissionens gennemførelsesafgørelse (EU) 2017/759 af 28. april 2017 om de fælles protokoller og dataformater, som luftfartsselskaberne skal benytte ved videregivelse af passagerlisteoplysninger (PNR-oplysninger) til passageroplysningsenhederne (PIU) (EUT L 113 af 29.4.2017, s. 48).

1.13. Nationale EES-adgangspunkter

Ind- og udrejsesystemet[29] (EES) sigter primært mod at forbedre forvaltningen af EU's ydre grænser og anvendes til dette formål af grænse-, indvandrings- og visummyndigheder[30]. Systemet registrerer elektronisk, hvornår og hvor visse tredjelandsstatsborgere, der er givet tilladelse til indrejse med henblik på et kortvarigt ophold på medlemsstaternes område, ind- og udrejser, og beregner varigheden af deres tilladte ophold. EES anvendes ved de ydre grænser. Medlemsstater, der anvender Schengenreglerne fuldt ud, indfører EES ved deres indre grænser med de medlemsstater, der endnu ikke anvender Schengenreglerne fuldt ud, men som enten anvender eller ikke anvender EES. Medlemsstater, der ikke anvender Schengenreglerne fuldt ud, indfører ingen biometriske funktioner.

Med hensyn til grænse-, indvandrings- og visummyndigheder kan nationale "udpegede myndigheder" søge i EES på de betingelser, der er fastsat i forordningen. De søger i det til retshåndhævelsesformål og for at muliggøre generering af oplysninger til efterforskning vedrørende terrorhandlinger eller andre alvorlige strafbare handlinger, herunder identifikationen af gerningsmænd, mistænke og ofre for disse lovovertrædelser, der har passeret de ydre grænser.

Medlemsstaterne udpeger de myndigheder, der har ret til at søge i EES til retshåndhævelsesformål. Desuden udpeger hver medlemsstat et centralt EES-adgangspunkt. Det centrale adgangspunkt er adskilt fra de "udpegede myndigheder", varetager sine opgaver fuldstændig uafhængigt af de "udpegede myndigheder" og bør ikke modtage instrukser fra dem med hensyn til udfaldet af kontrollen, dvs. processen med at sammenligne datasæt for at fastslå gyldigheden af en påstået identitet, så det sikres, at den udføres uafhængigt. Kun behørigt bemyndiget personale hos det centrale adgangspunkt har ret til at få adgang til EES.

---

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

[30] Kommissionen bestemmer, fra hvilken dato EES skal idriftsættes, når betingelserne i artikel 66 i forordning (EU) 2017/2226 er opfyldt.

Operative enheder inden for de "udpegede myndigheder" har ret til at anmode om oplysninger i EES gennem de centrale adgangspunkter. Med henblik herpå skal den operative enhed indgive en begrundet elektronisk eller skriftlig anmodning til et centralt adgangspunkt om adgang til oplysninger i EES. Det centrale adgangspunkt kontrollerer, om adgangsbetingelserne i henhold til forordningen er opfyldt, og behandler i så fald anmodningen. Oplysningerne fra EES sendes derefter til en operativ enhed på en sådan måde, at datasikkerheden ikke bringes i fare.

Følgende betingelser skal kontrolleres for at få adgang til oplysninger fra EES til retshåndhævelsesformål:

- adgang til søgning er nødvendig til retshåndhævelsesformål
- adgang til søgning er nødvendig og står i et rimeligt forhold til formålet i en bestemt sag
- der er bevis for eller rimelige grunde til at antage, at søgningen i oplysninger i EES vil bidrage til at forebygge, afsløre eller efterforske en af de pågældende strafbare handlinger, navnlig når der er begrundet mistanke om, at den mistænkte, gerningsmanden eller offeret for en terrorhandling eller en anden alvorlig strafbar handling falder ind under en kategori, der er omfattet af denne forordning.

Desuden gives der adgang til EES med henblik på at identificere den mistænkte, gerningsmanden eller offeret for sådanne lovovertrædelser, hvis

- der er foretaget en forudgående søgning i nationale databaser
- for så vidt angår søgninger med fingeraftryk, der er iværksat en forudgående søgning i henhold til Rådets afgørelse 2008/615/RIA ("Prümafgørelsen"), hvor det er teknisk muligt at foretage sammenligninger af fingeraftryk, og den pågældende søgning enten er fuldt ud gennemført, eller den pågældende søgning ikke er fuldt ud gennemført senest to dage efter dens iværksættelse.

En anmodning om søgning i VIS vedrørende den samme registrerede kan indgives sideløbende med anmodningen om søgning i EES i henhold til betingelserne i Rådets afgørelse 2008/633/RIA[31].

Endelig gives der adgang til EES med henblik på søgning i rejsehistorikken eller oplysninger om opholdsperioder på medlemsstaternes område for en kendt mistænkt, en kendt gerningsmand eller et kendt formodet offer for en terrorhandling eller en anden alvorlig strafbar handling, når ovennævnte principper er opfyldt.

1.14. National ETIAS-enhed[32]

Det europæiske system vedrørende rejseinformation og rejsetilladelse (ETIAS) støtter[33] informationsudveksling med henblik på grænseforvaltning, retshåndhævelse og bekæmpelse af terrorisme. ETIAS har til formål at fastlægge, hvorvidt tredjelandsstatsborgere, der er fritaget for visumpligt, opfylder betingelserne herfor, inden de rejser til Schengenområdet og forud for deres ankomst til grænseovergangssteder ved de ydre grænser. ETIAS giver en rejsetilladelse, der er af en anden karakter end et visum, men som udgør en betingelse for indrejse og ophold, og angiver, at ansøgeren ikke udgør en risiko for sikkerheden, en risiko for ulovlig indvandring eller en høj risiko for epidemi.

ETIAS består af:

- ETIAS-informationssystemet, herunder ETIAS-overvågningslisten
- den centrale ETIAS-enhed, som er del af Det Europæiske Agentur for Grænse- og Kystbevogtning
- de nationale ETIAS-enheder.

---

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

32 Europa-Parlamentets og Rådets forordning (EU) 2018/1240 af 12. september 2018 om oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) og om ændring af forordning (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399 (EU) 2016/1624 og (EU) 2017/2226 (EUT L 236 af 19.9.2018, s. 1).
Europa-Parlamentets og Rådets forordning (EU) 2018/1241 af 12. september 2018 om ændring af forordning (EU) 2016/794 med henblik på oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) (EUT L 236 af 19.9.2018, s. 72).

33 Kommissionen bestemmer, fra hvilken dato EES skal idriftsættes, når betingelserne i artikel 88 i forordning (EU) 2018/1240 er opfyldt.

Hvis den automatiserede ansøgningsproces viser, at der er en overensstemmelse ("hit") mellem oplysninger i ansøgningsmappen og oplysningerne i ETIAS-informationssystemerne, specifikke risikoindikatorer eller indberetninger i de EU-informationssystemer, der søges i, har den centrale ETIAS-enhed til opgave at kontrollere dette hit og, hvis en overensstemmelse bekræftes, eller hvis der fortsat hersker tvivl, iværksætte den manuelle behandling af ansøgningen i den identificerede medlemsstat.

Efterfølgende er det den pågældende medlemsstats nationale ETIAS-enhed, der manuelt behandler den pågældende ansøgning. Den vil få adgang til ansøgningsmappen og eventuelt tilknyttede ansøgningsmapper såvel som til eventuelle hit, der blev udløst under den automatiserede behandling. Efter manuel behandling udsteder eller afviser den ansvarlige nationale enhed i sidste ende en rejsetilladelse i overensstemmelse med forordningens bestemmelser. Til dette formål kan den nationale enhed anmode om yderligere oplysninger eller dokumentation.

Der skal gives afslag på rejsetilladelse, hvis ansøgeren:

- anvender et rejsedokument, der er blevet meldt bortkommet, stjålet, uretmæssigt tilegnet eller ugyldiggjort i SIS
- udgør en risiko for sikkerheden
- udgør en risiko for ulovlig indvandring
- udgør en høj risiko for epidemi
- er en person, der er indberettet til SIS med henblik på nægtelse af indrejse eller ophold
- ikke svarer på en anmodning om yderligere oplysninger eller dokumentation eller ikke møder op til en samtale.

De nationale ETIAS-enheder er ansvarlige for at behandle ansøgninger og afgøre, om der skal udstedes en rejsetilladelse eller ej, eller om en rejsetilladelse skal annulleres eller inddrages. Med henblik herpå bør de nationale enheder samarbejde med hinanden og med Europol med henblik på at vurdere ansøgninger.

En national enhed kan beslutte at afslå en rejsetilladelse, annullere en rejsetilladelse, hvis det bliver åbenlyst, at betingelserne for at udstede den ikke var opfyldt på tidspunktet for udstedelsen, eller inddrage en rejsetilladelse, hvis det bliver åbenlyst, at betingelserne for at udstede den ikke længere er opfyldt. De berørte ansøgere har ret til at påklage afgørelsen. Klagesager skal føres i den medlemsstat, der har truffet afgørelse om afslaget, annulleringen eller inddragelsen, i henhold til den pågældende medlemsstats nationale ret. Den kompetente nationale enhed har til opgave at underrette ansøgere om klageproceduren.

Grænsemyndigheder, der har kompetence til at foretage kontrol ved overgangssteder ved de ydre grænser, søger i det centrale ETIAS-system ved anvendelse af oplysningerne i den maskinlæsbare del af rejsedokumentet. Indvandringsmyndighederne, der kontrollerer eller verificerer, om betingelserne for indrejse eller ophold på medlemsstaternes område er opfyldt, har adgang til at søge i ETIAS' centrale system.

Kun i særlige tilfælde, og kun når det er nødvendigt for at forebygge, afsløre eller efterforske terrorhandlinger eller alvorlige strafbare handlinger, har de udpegede retshåndhævende myndigheder i medlemsstaterne ret til at anmode om søgning i de personoplysninger, der er registreret i det centrale ETIAS-system. Direktiv (EU) 2016/680 ("politidirektivet") finder anvendelse på de af medlemsstaterne udpegede myndigheders behandling af sådanne personoplysninger i henhold til ETIAS-forordningen.

1.15. Interoperabilitet

Hovedformålet med "interoperabilitetspakken"[34] er at forbedre Unionens dataforvaltningsstruktur for grænseforvaltning og sikkerhed, så det bliver lettere at foretage en korrekt identifikation af personer, som ikke er EU-borgere, men tredjelandsstatsborgere. Formålet med interoperabilitet mellem EES (se punkt 3.18), VIS (se punkt 3.7), ETIAS (se punkt 3.19), Eurodac (se punkt 3.8), SIS (se punkt 3.2) og ECRIS-TCN (se punkt 3.13.2) er at gøre det muligt for disse EU-informationssystemer at supplere hinanden. Med henblik herpå oprettes en europæisk søgeportal (ESP), en fælles biometrisk matchtjeneste, et fælles identitetsregister og en multiidentitetsdetektor[35].

a) For at sikre systematisk brug af ovennævnte EU-informationssystemer bør de udpegede myndigheder, der har ret til at få adgang til mindst én af dem, det fælles identitetsregister og multiidentitetsdetektoren, til Europol-oplysninger eller til INTERPOL's SLTD- og TDAWN-database (se punkt 2.4), anvende ESP, som gør det muligt at søge samtidigt i disse informationssystemer.

b) Det fælles identitetsregister opretter en individuel sagsmappe for hver person, der er registreret i disse informationssystemer, og forstås som et fælles register over identitetsdata, rejsedokumentoplysninger og biometriske data for personer, der er registreret i systemerne. Det fælles identitetsregister bør være en del af systemernes tekniske struktur og fungere som en fælles komponent mellem dem til lagring og søgning af de identitetsdata, rejsedata og biometriske data, de behandler.

---

[34] Europa-Parlamentets og Rådets forordning (EU) 2019/817 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende grænser og visum og om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 og (EU) 2018/1861, Rådets beslutning 2004/512/EF og Rådets afgørelse 2008/633/RIA (EUT L 135 af 22.5.2019, s. 27).
Europa-Parlamentets og Rådets forordning (EU) 2019/818 af 20. maj 2019 om fastsættelse af en ramme for interoperabilitet mellem EU-informationssystemer vedrørende politisamarbejde og retligt samarbejde, asyl og migration og om ændring af forordning (EU) 2018/1726, (EU) 2018/1862 og (EU) 2019/816 (EUT L 135 af 22.5.2019, s. 85).

[35] Kommissionen fastsætter den dato, hvorfra bestemmelserne i forordningerne vedrørende ESP, den fælles biometriske matchtjeneste, det fælles identitetsregister og multiidentitetsdetektoren finder anvendelse.

Adgang til det fælles identitetsregister gives med henblik på f.eks.

- korrekt identifikation af den person, der er registreret i EU-informationssystemerne, eller om nødvendigt

- for at bistå de retshåndhævende myndigheder med forebyggelse, afsløring og efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger.

Hvis en politimyndighed af en række forskellige årsager ikke er i stand til at identificere en person, kan denne myndighed søge i det fælles identitetsregister. Med henblik herpå giver medlemsstaterne på grundlag af den nationale lovgivning deres kompetente myndighed beføjelse til at gøre dette og fastlægger procedurer, betingelser og kriterier for en sådan kontrol. Forespørgslen udføres enten på grundlag af friske fingeraftryk af den pågældende person eller, hvis dette ikke kan lade sig gøre, på grundlag af identitetsdata om personen i kombination med rejsedokumentoplysninger.

Hvis forespørgslen viser, at data om den pågældende person er lagret i det fælles identitetsregister, får politimyndigheden efternavn, fornavn, fødselsdato, fødested, nationalitet, køn, eventuelle tidligere navne, pseudonymer eller kaldenavne samt, hvis de forefindes, oplysninger på rejsedokumenter. Politiet kan endvidere, hvis det er berettiget i henhold til national lovgivning, foretage biometriske søgninger i det fælles identitetsregister i tilfælde af en naturkatastrofe, en ulykke eller et terrorangreb og udelukkende med henblik på at identificere ukendte personer, som er ude af stand til at identificere sig selv, eller uidentificerede jordiske rester.

Søgning i det fælles identitetsregister til retshåndhævelsesformål, navnlig hvis der er mistanke om, at den mistænkte, gerningsmanden eller offeret for en terrorhandling eller grov kriminalitet er en person, hvis oplysninger er lagret i informationssystemerne, kan de udpegede myndigheder og Europol søge i det fælles identitetsregister for at konstatere, om der lagres oplysninger om en bestemt person. I bekræftende fald bestemmer det fælles identitetsregister efter automatiseret kontrol af, at der er et match i systemet ("match flag"-funktion), et svar i form af en reference, der angiver, hvilket informationssystem der indeholder de matchende data. Svaret af "match flag"-typen bør kun anvendes med henblik på at indgive en anmodning om adgang til det underliggende EU-informationssystem. Et sådant svar må ikke afsløre personoplysninger om den pågældende person ud over at angive, at oplysningerne er lagret i et af systemerne.

Den autoriserede slutbruger bør ikke træffe nogen negativ afgørelse vedrørende den pågældende person alene på grundlag af forekomsten af en hit-påtegning. Slutbrugerens adgang til et "match flag" formodes derfor at udgøre et meget begrænset indgreb i retten til at beskytte personoplysninger om den pågældende person, samtidig med at de udpegede myndigheder får mulighed for at anmode om adgang til personoplysninger mere effektivt. Fuld adgang til data til retshåndhævelsesformål er underlagt de betingelser og procedurer, der er fastsat i Eurodacforordningen (se punkt 2.7).

c) Multiidentitetsdetektoren (MID) opretter og lagrer links mellem oplysninger i de forskellige EU-informationssystemer. For retshåndhævelse: Multiidentitetsdetektoren i det fælles identitetsregister og SIS igangsættes, hvis der oprettes eller ajourføres en SIS-indberetning om en person, eller hvis der oprettes eller ændres en datapost i ECRIS-TCN. Den igangsættes kun med henblik på at sammenligne oplysninger i ét EU-informationssystem med oplysninger, der er tilgængelige i et andet EU-informationssystem. Kontrollen af de forskellige identiteter foretages manuelt af henholdsvis det pågældende SIRENE-kontor eller de respektive centrale myndigheder.

Kommissionen:

- fastsætter den dato, hvorfra bestemmelserne i forordningerne vedrørende ESP, den fælles biometriske matchtjeneste, det fælles identitetsregister og multiidentitetsdetektoren finder anvendelse

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

1.16. Valg af kanal - almindeligt anvendte kriterier

I en medlemsstat spiller SPOC'et[36] en afgørende rolle ved fastlæggelsen af den mest hensigtsmæssige og relevante kanal ved at samle alle anmodninger (både indkommende og udgående), som enheden behandler. Nationale myndigheder giver af effektivitetshensyn efterforskerne en betydelig grad af autonomi med hensyn til valg af den efterforskningskanal, der skønnes mest hensigtsmæssig. De mest almindeligt anvendte kommunikationskanaler er følgende:

[36] Retningslinjer for et enkelt kontaktpunkt (SPOC) (10492/14 DAPIX 75 ENFOPOL 157 og 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1).

- SIRENE gennem hver Schengenstats kontaktpunkter for SIS
- Europol gennem Europols nationale enheder/Europols forbindelsesofficerer
- INTERPOL gennem de nationale centralbureauer i de nationale politihovedkvarterer
- forbindelsesofficerer
- kanaler for gensidig bistand, der anvendes mellem toldmyndigheder (Napoli II)
- bilaterale kanaler på grundlag af samarbejdsaftaler på nationalt, regionalt og lokalt plan (PCCC'er).

Ifølge de generelle regler sendes en anmodning kun gennem én kanal. I ekstraordinære tilfælde kan der imidlertid sendes en anmodning gennem forskellige kanaler på samme tid. I sådanne tilfælde bør alle parter behørigt underrettes herom på en hensigtsmæssig måde. En kanalændring bør på samme måde meddeles alle parter sammen med begrundelsen herfor.

For at undgå emnemæssige sammenfald eller situationer, hvor en anmodning sendes unødigt mere end én gang gennem forskellige kanaler, kan den relevante sagsbehandler (SIS, Europol, INTERPOL, bilateral forbindelsesofficer) i den anmodende stat fastsætte, hvordan en anmodning om oplysninger sendes på den mest hensigtsmæssige måde på grundlag af følgende kriterier:

- geografiske kriterier, dvs. den berørte persons eller genstands nationalitet/opholdssted/oprindelse er bekendt, og anmodningen vedrører meddelelse af nærmere oplysninger (adresse, telefonnummer, fingeraftryk, DNA, registrering osv.)
- tematiske kriterier, dvs. organiseret kriminalitet, grov kriminalitet og terrorisme fortrolighed/følsomhed benyttet kanal i forbindelse med en tidligere lignende anmodning
- tekniske kriterier: dvs. behovet for sikre IT-kanaler
- uopsættelighedskriterier, dvs. en umiddelbar risiko for en persons fysiske integritet, øjeblikkeligt tab af beviser, anmodning om presserende grænseoverskridende operationer eller overvågning.

2. INFORMATIONSSYSTEMER

2.1. Schengeninformationssystemet - anden generation (SIS II)[37]

For øjeblikket er anden generation af Schengeninformationssystemet ("SIS II") i drift i 26 EU-medlemsstater samt i de fire ikke-EU-lande, der er associeret til Schengensamarbejdet: Norge, Island, Schweiz og Liechtenstein. Det støtter det operationelle samarbejde mellem politimyndigheder og judicielle myndigheder i straffesager. Da SIS er et system for både politisamarbejde og grænsekontrol, kan udpegede politifolk, grænsevagter, toldere og visummyndigheder samt judicielle myndigheder i hele Schengenområdet konsultere SIS[38].

Der kan søges i SIS II-oplysninger (under overholdelse af strenge databeskyttelsesregler) døgnet rundt/alle dage via adgangspunkter i SIRENE-kontorerne, ved grænsekontrolsteder, inden for nationalt territorium og på konsulater i udlandet. I databasen registreres oplysninger om både **personer** og **genstande**, og den muliggør udveksling af oplysninger med henblik på forebyggelse af kriminalitet og bekæmpelse af irregulær indvandring. Den person, der foretager undersøgelsen, kan hurtigt gennem onlinesøgninger i SIS fastslå - ud fra et princip om "hit/no hit" - om den person, der kontrolleres, nævnes i databasen eller ej.

Der henvises til oplysninger som indberetninger, hvor en indberetning er et sæt oplysninger, der gør det muligt for myndighederne at identificere personer eller genstande med henblik på at træffe passende forholdsregler:

Indberetninger om **personer** rettet mod både EU-borgere og ikke-EU-borgere. Disse anvendes til at træffe foranstaltninger som:

- anholdelse med henblik på overgivelse på baggrund af enten den europæiske arrestordre eller aftaler indgået mellem EU og tredjelande eller anholdelse med henblik på udlevering
- søgning efter forsvundne personer, hvis opholdssted er ubekendt
- stævning om fremmøde for en domstol som led i en straffesag eller fuldbyrdelse af en dom, der involverer frihedsberøvelse

---

37 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).

38 En liste over de kompetente nationale myndigheder, der har ret til adgang til indberetninger offentliggøres hvert år i *Den Europæiske Unions Tidende*.

– diskret kontrol og målrettet kontrol med henblik på retsforfølgning af strafbare handlinger og forebyggelse af trusler mod den offentlige eller nationale sikkerhed

– nægtelse af indrejse til Schengenområdet for statsborgere eller tredjelandsstatsborgere som resultat af en administrativ afgørelse eller retsafgørelse eller på grund af en trussel mod den offentlige orden eller den nationale sikkerhed eller på grund af manglende overholdelse af nationale bestemmelser for udlændinges indrejse og opholdssted.

SIS II-indberetninger om **genstande** indlæses med henblik på diskret eller målrettet kontrol, beslaglæggelse, anvendelse som bevis i straffesager eller overvågning. Disse indberetninger kan omhandle:

– motorkøretøjer, både, luftfartøjer, containere

– skydevåben

– stjålne dokumenter

– pengesedler

– stjålne genstande som kunstgenstande, både og skibe.

Særligt bemyndiget Europolpersonale har inden for rammerne af sit mandat ret til adgang til og søgning direkte i oplysninger, der er indlæst i SIS II, og kan anmode om yderligere oplysninger fra den berørte medlemsstat.

De nationale medlemmer af Eurojust og deres assistenter har inden for rammerne af deres mandat ret til adgang til og søgning i oplysninger, der er indlæst i SIS II.

2.2. Europols informationssystem (EIS)[39]

Europolforordningen introducerer et nyt databehandlingskoncept, som almindeligvis benævnes det integrerede datastyringskoncept (Integrated Data Management Concept (IDMC)). IDMC kan defineres som muligheden for at anvende oplysninger vedrørende kriminalitet til flere forskellige forretningsformål som anført af dataejeren, hvilket giver mulighed for at administrere og behandle dem på en integreret, teknologineutral måde. I Rådets Europolafgørelse var databehandlingen struktureret omkring systemer. Europolforordningen indeholder ikke længere henvisninger til systemer, men stiller i stedet krav om angivelse af formålet med behandlingen. For at lette overgangen kan brugere fortsat arbejde med de eksisterende systemer på en måde, der er i overensstemmelse med den nye retlige ramme.

Europols informationssystem (EIS), som der henvises til i Europolafgørelsen, er et centraliseret system hos Europol, der gør det muligt for medlemsstaterne og Europols samarbejdspartnere at lagre, dele og krydstjekke oplysninger vedrørende mistænkte, domfældte eller "potentielle fremtidige kriminelle", der er involveret i kriminalitet, som er omfattet af Europols mandat (grov kriminalitet, organiseret kriminalitet eller terrorisme). Systemet muliggør lagring af alle typer oplysninger og beviser vedrørende denne kriminalitet/disse personer, f.eks. personer med kaldenavne, selskaber, telefonnumre, e-mailadresser, motorkøretøjer, våben, DNA, foto, fingeraftryk, bomber osv. EIS, som i første omgang tjener som det system, der understøtter krydstjek, giver en hit/no hit-adgang. Europolforordningen fastsætter, at der er fuld adgang til oplysninger, der er indgivet med henblik på analyser af strategisk eller tematisk art, men kun hit/no hit-adgang til oplysninger, der er leveret med henblik på operationel analyse.

EIS fungerer reelt som et referencesystem, der hjælper med at fastslå, om de oplysninger, der søges efter, er tilgængelige i en af EU's medlemsstater, hos samarbejdspartnere eller hos Europol. Systemet er direkte tilgængeligt i alle medlemsstater og for alle behørigt bemyndigede medlemmer af Europolpersonalet. På nuværende tidspunkt kan der skelnes mellem tre måder for medlemsstaterne at uploade oplysninger på:

a) manuel indtastning af oplysninger i EIS eller via SIENA

---

[39] 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) (gældende fra 1. maj 2017).

b) halvautomatisk overførsel ved at foretage en batchuploading i EIS

c) automatisk dataoverførsel ved hjælp af et dataindlæsningsprogram.

Langt de fleste oplysninger i EIS indlæses ved hjælp af automatiske dataindlæsningssystemer. Medlemsstaternes tilgang til dataindsamling har ændret sig, idet fokus ved overførsel af oplysninger har flyttet sig til enheder, der kan krydsmatches, som personer, biler, telefonnumre og våben.

Tredjelande kan ikke indføre eller krydstjekke oplysninger direkte i EIS, men i henhold til artikel 23, stk. 5, i Europolforordningen kan de indgive dem til Europol. Europol vil først skulle vurdere, om oplysningerne falder inden for dets mandat, og kan først derefter acceptere oplysningerne og foretage et krydstjek af oplysningerne.

EIS, som muliggør deling af yderst følsomme oplysninger, har et robust system, der sikrer fortrolighed og sikkerhed. Sikkerheden garanteres bl.a. af de specifikke håndteringskoder. De viser, hvad der kan gøres med de givne oplysninger, og hvem der har adgang til dem. Håndteringskoderne er udarbejdet med henblik på at beskytte informationskilderne og sikre, at behandling af oplysningerne sker i overensstemmelse med de ønsker, som ejeren af oplysningerne måtte have, og i overensstemmelse med medlemsstatens nationale ret. EIS er akkrediteret til behandling af informationer op til og med RESTREINT UE/EU RESTRICTED.

2.3. Europols netværksprogram til sikker informationsudveksling (SIENA)

SIENA er Europols sikre kommunikationssystem, som medlemsstaterne, Europol og Europols samarbejdspartnere anvender til udveksling af operationelle og strategiske oplysninger og efterretninger vedrørende kriminalitet, herunder operationelle data om personer. SIENA er et meddelelsessystem, der tilbyder forskellige meddelelsestyper til forskellige formål, herunder udveksling af oplysninger i overensstemmelse med den "svenske rammeafgørelse".

Der blev ved udformningen og i funktionaliteten af SIENA lagt betydelig vægt på sikkerhed, databeskyttelse og fortrolighed. SIENA er blevet akkrediteret til udveksling af oplysninger, der er klassificeret som CONFIDENTIEL UE/EU CONFIDENTIAL. Udveksling af oplysninger gennem SIENA indebærer et klart databehandlingsansvar. Der skal angives klassifikationsniveau (fortrolighed), håndteringskoder og kildens og oplysningernes pålidelighed for hver enkelt SIENA-meddelelse, der udsendes.

Standardsproget for SIENA-brugergrænsefladen er engelsk, mens grænsefladen er flersproget, så SIENA-operatører kan arbejde på deres eget eller egne nationale sprog. Ud over at udveksle meddelelser kan SIENA-operatører foretage søgninger og udarbejde statistiske rapporter om de oplysninger, der udveksles gennem SIENA.

SIENA støtter bilateral udveksling af oplysninger mellem medlemsstater og gør det muligt for dem at udveksle oplysninger uden for Europols mandat. Ved henvendelse til en af Europols samarbejdspartnere i forbindelse med udvekslingen af oplysninger underrettes medlemsstaterne via SIENA om, at denne udveksling kun bør finde sted, hvis den vedrører kriminalitet inden for Europols mandat.

Europol håndterer kun oplysninger, der udveksles via SIENA, med henblik på operationel databehandling, hvis Europol er en af adressaterne i udvekslingen af oplysninger. Med henblik på revision er alle oplysninger, der udveksles via SIENA, tilgængelige for Europols databeskyttelsesansvarlige og de nationale tilsynsmyndigheder.

SIENA støtter udveksling af strukturerede oplysninger, der er baseret på det universelle meddelelsesformat UMF. I øjeblikket kan UMF PERSON-enheden skabes/vises i selve SIENA-webapplikationen. Den fuldstændige UMF-datamodel understøttes allerede af SIENA-webtjenesten.

2.4. INTERPOL's globale politikommunikationssystem (I-24/7)

Det globale netværk til udveksling af politioplysninger I-24/7 forbinder INTERPOL's Generalsekretariat i Lyon, Frankrig, de nationale centralbureauer (NCB) i 190 lande og de regionale kontorer.

INTERPOL's informationssystem muliggør direkte kommunikation i form af meddelelser mellem NCB'er. Alle INTERPOL-databaser (med undtagelse af databasen med billeder af seksuel udnyttelse af børn) er tilgængelige i realtid via det globale politikommunikationssystem I-24/7. I-24/7-systemet giver også medlemslandene mulighed for at få adgang til hinandens nationale databaser med en business to business-forbindelse (B2B). Medlemslandene forvalter og opbevarer deres egne nationale oplysninger om kriminalitet og kontrollerer indsendelse heraf, andre landes adgang hertil og tilintetgørelse af oplysninger i overensstemmelse med deres nationale lovgivning. De har også mulighed for at gøre dem tilgængelige for det internationale retshåndhævelsessamfund gennem I-24/7.

2.4.1. INTERPOL: DNA-gateway

INTERPOL's DNA-database omfatter en international DNA-database, en formular til anmodning om internationale søgninger i forbindelse med bilateral udveksling og en metode til sikker og standardiseret elektronisk overførsel. Der opbevares ingen nominaldata, der forbinder en DNA-profil med en person. DNA-gatewayen er kompatibel med elektronisk dataudveksling i henhold til Prüm.

Medlemslandene kan få adgang til databasen, og adgangen kan efter anmodning udvides til ud over medlemslandenes nationale centralkontorer at omfatte kriminaltekniske centre og laboratorier. Politi i medlemslandene kan indsende DNA-profiler fra lovovertrædere, gerningssteder, forsvundne personer og uidentificerede lig.

2.4.2. INTERPOL's fingeraftryksdatabase

Autoriserede brugere i medlemslandene kan se, indsende og krydstjekke registreringer via et automatisk fingeraftryksidentifikationssystem (AFIS) Registreringerne gemmes og udveksles i et format, som fastsættes af National Institute of Standards and Technology (NIST). Dokumenterne Guidelines concerning Fingerprints Transmission og Guidelines concerning transmission of Fingerprint Crime Scene Marks hjælper medlemslandene med at forbedre kvaliteten og kvantiteten af de fingeraftryk, der indsendes til INTERPOL's AFIS.

2.4.3. INTERPOL's database over stjålne og bortkomne rejsedokumenter

INTERPOL's database over stjålne og bortkomne rejsedokumenter indeholder oplysninger om mere end 45 mio. rejsedokumenter, som 166 lande har meldt tabt eller stjålet. Denne database gør det muligt for INTERPOL's NCB'er og andre autoriserede retshåndhævende organer (som f.eks. personale i indvandrings- og grænsekontrolmyndigheder) at vurdere gyldigheden af et mistænkeligt rejsedokument. Med henblik på at forhindre og bekæmpe grov og organiseret kriminalitet udveksler medlemsstaternes kompetente retshåndhævende myndigheder pasoplysninger med INTERPOL[40].

2.4.4. Rejsedokumenter med tilknyttede notifikationer (TDAWN)

TDAWN-databasen indeholder oplysninger om rejsedokumenter, der er knyttet til personer, som er omfattet af en efterlysning via INTERPOL.

2.4.5. Referencetabel over skydevåben

Ved brug af INTERPOL's referencetabel over skydevåben kan efterforskere korrekt identificere et skydevåben (fabrikat, model, kaliber osv.). Den indeholder mere end 250 000 henvisninger til skydevåben og 57 000 højkvalitetsfotos. INTERPOL's ballistikinformationsnet er en platform for omfattende international deling og sammenligning af ballistiske data og indeholder mere end 150 000 registreringer.

INTERPOL's system til registrering og sporing af ulovlige skydevåben (iARMS) er en informationsteknologisk applikation, som letter de retshåndhævende myndigheders udveksling af oplysninger og samarbejde om skydevåbenrelateret kriminalitet.

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

2.5. Det europæiske informationssystem vedrørende strafferegistre (ECRIS)[41]

Det IT-baserede europæiske informationssystem vedrørende strafferegistre (ECRIS)[42] er det elektroniske værktøj, som benyttes til udveksling af oplysninger vedrørende domme mellem medlemsstaterne i et standardiseret format. ECRIS anvendes til at underrette medlemsstaterne om deres statsborgeres straffedomme og til at sende anmodninger om oplysninger om straffedomme med henblik på straffesager og andre formål såsom administrative eller ansættelsesmæssige formål. Der kan ligeledes foretages anmodninger vedrørende tredjelandsstatsborgere, hvis der er grund til at antage, at den anmodede medlemsstat har oplysninger om den pågældende person.

ECRIS-anmodninger skal besvares inden for 10 arbejdsdage, hvis anmodningen vedrører enten straffesager eller ansættelsesmæssige formål, og inden for 20 arbejdsdage, hvis anmodningen er fremsat af en fysisk person vedrørende egne oplysninger.

ECRIS er ikke udformet til at fungere som en centraliseret database over strafferegistre, men er baseret på en decentral IT-arkitektur, hvorved alle strafferegistre udelukkende lagres i databaser, som drives af medlemsstaterne. Oplysningerne udveksles elektronisk mellem medlemsstaternes udpegede centrale myndigheder.

Medlemsstaterne overfører oplysningerne i overensstemmelse med de vedtagne regler og standardformater, og de skal være så fuldstændige som muligt for at gøre det muligt for den modtagende medlemsstat at behandle oplysningerne ordentligt og identificere personen. Meddelelserne sendes på de berørte medlemsstaters officielle sprog eller på et andet sprog, som begge medlemsstater accepterer.

---

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

42 Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 171 af 7.6.2019, s. 143, EUT L 151 af 7.6.2019, s. 143).

Rådets Generalsekretariat har offentliggjort en ikkebindende håndbog for praktikere, der beskriver procedurerne for udveksling af procedurer og koordinerer tiltag til udvikling af drift af ECRIS, og som er tilgængelig i elektronisk format på Rådets websted og på Europa-Kommissionens websted CIRCABC på https://circabc.europa.eu. Anmodninger om adgang til håndbogen sendes til Rådssekretariatet. Anmodninger om adgang til den begrænsede interessegruppe "ECRIS Business and Technical Support" sendes til Europa-Kommissionen.

2.5.1. ECRIS-TCN[43]

Den retlige ramme for ECRIS tager ikke i tilstrækkelig grad højde for alle forhold eller anmodninger vedrørende tredjelandsstatsborgere. I Unionen indsamles oplysninger om tredjelandsstatsborgere ikke, som det er tilfældet for medlemsstaternes statsborgere, men lagres udelukkende i de medlemsstater, hvor straffedommene er afsagt. Ved hjælp af ECRIS-TCN[44] kan den centrale nationale myndighed finde ud af, hvilke andre medlemsstater der ligger inde med strafferegisteroplysninger om en tredjelandsstatsborger. ECRIS-rammen kan derefter anvendes til at anmode disse medlemsstater om sådanne oplysninger i overensstemmelse med rammeafgørelse 2009/315/RIA.

Forordningen fastsætter regler om oprettelse af et centralt system på EU-plan med personoplysninger og regler om ansvarsfordelingen mellem medlemsstaten og den organisation, der er ansvarlig for udvikling og vedligeholdelse af det centraliserede system. Den fastsætter et passende samlet niveau for databeskyttelse, datasikkerhed og beskyttelse af de berørte personers grundlæggende rettigheder.

---

[43] Europa-Parlamentets og Rådets forordning (EU) 2019/816 af 17. april 2019 om oprettelse af et centralt system til bestemmelse af, hvilke medlemsstater der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer (ECRIS-TCN) for at supplere det europæiske informationssystem vedrørende strafferegistre, og om ændring af forordning (EU) 2018/1726 (EUT L 135 af 22.5.2019, s. 1).
Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 171 af 7.6.2019, s. 143).

[44] Kommissionen bestemmer, fra hvilken dato ECRIS-TCN skal idriftsættes, når betingelserne i artikel 35 i forordning (EU) 2019/816 er opfyldt.

Medlemsstaterne bør i ECRIS-TCN oprette en datapost for domfældte tredjelandsstatsborgere. Dette bør, hvor det er muligt, ske automatisk og uden unødig forsinkelse efter indlæsningen af deres straffedom i det nationale strafferegister. Medlemsstaterne bør i overensstemmelse med forordningen indlæse alfanumeriske oplysninger og fingeraftryksoplysninger i det centrale system vedrørende straffedomme afsagt efter datoen for påbegyndelsen af indlæsning af oplysninger i ECRIS-TCN. Fra samme dato og på et hvilket som helst tidspunkt derefter bør medlemsstaterne kunne indlæse ansigtsbilleder i det centrale system.

ECRIS-TCN muliggør behandling af fingeraftryksoplysninger med henblik på at bestemme, hvilke medlemsstater der ligger inde med strafferegisteroplysninger om en tredjelandsstatsborger. Det bør også muliggøre behandling af ansigtsbilleder for at kunne bekræfte vedkommendes identitet. Det er afgørende, at indlæsningen og anvendelsen af fingeraftryksoplysninger og ansigtsbilleder ikke går videre, end hvad der er strengt nødvendigt for at nå målet, respekterer de grundlæggende rettigheder samt børns tarv og er i overensstemmelse med gældende EU-databeskyttelsesregler.

Eurojust, Europol, og EPPO bør have adgang til ECRIS-TCN med henblik på at kunne bestemme, hvilke medlemsstater der ligger inde med strafferegisteroplysninger om en tredjelandsstatsborger, for at støtte dem i udførelsen af deres lovbestemte opgaver.

Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) står for udvikling og drift af ECRIS-TCN.

2.6. Visuminformationssystemet (VIS)[45]

Visuminformationssystemet (VIS) er først og fremmest et indrejsekontrolsystem. Det er et redskab, der anvendes til at lette søgning på konsulat- og grænsekontrolplan gennem elektronisk kontrol og udveksling af visumoplysninger mellem medlemsstaterne. Som sådan er det rettet mod visumpligtige udenlandske statsborgere. Medlemsstaternes udpegede myndigheder (dvs. konsulære repræsentationer, grænsekontrolsteder, politi og indvandringsmyndigheder)[46] og Europol[47], inden for rammerne af sine opgaver, har mulighed for at søge i VIS[48] med henblik på forebyggelse, afsløring og efterforskning af:

- terrorhandlinger, dvs. lovovertrædelser i national ret, der svarer til eller er ligestillet med de strafbare handlinger i artikel 1-4 i Rådets rammeafgørelse 2002/475/RIA af 13. juni 2002 om bekæmpelse af terrorisme, og

- alvorlige strafbare handlinger, dvs. de former for kriminalitet, der svarer til eller er ligestillet med dem, der er omhandlet i artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA ("den europæiske arrestordre").

---

45 Rådets beslutning af 8. juni 2004 om indførelse af visuminformationssystemet (VIS) (2004/512/EF) (EUT L 213 af 15.6.2004, s. 5).

46 Liste over kompetente myndigheder, hvis behørigt bemyndigede medarbejdere har adgang til at indlæse, ændre, slette eller søge oplysninger i visuminformationssystemet (VIS) (EUT C 187 af 26.5.2016, s. 4).

47 Rådets afgørelse 2008/633/RIA af 23. juni 2008 om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (EUT L 218 af 13.8.2008, s. 129). Rådets afgørelse 2013/392/EU af 22. juli 2013 om fastsættelse af den dato, fra hvilken afgørelse 2008/633/RIA om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger har virkning (EUT L 198 af 23.7.2013, s. 392).

48 EU-Domstolen annullerede den 16. april 2015 Rådets afgørelse 2013/392/EU af 22. juli 2013 om fastsættelse af den dato, fra hvilken afgørelse 2008/633/RIA om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger har virkning. Domstolen erklærede dog, at virkningerne af afgørelse 2013/392/EU opretholdes indtil ikrafttrædelsen af en ny retsakt, der erstatter den.

I henhold til den svenske rammeafgørelse kan oplysninger i VIS videregives til Det Forenede Kongerige og Irland af de kompetente myndigheder i de medlemsstater, hvis udpegede myndigheder har adgang til VIS, og oplysninger i Det Forenede Kongeriges og Irlands nationale visumregistre kan videregives til de kompetente retshåndhævende myndigheder i de øvrige medlemsstater.

VIS er baseret på en centraliseret arkitektur og en fælles platform med SIS II. VIS-data behandles i to trin. På første trin består data af alfanumeriske data og fotografier. På andet trin behandles biometriske data og scannede dokumenter, og de indføres i VIS. VIS indeholder oplysninger om visumansøgninger, fotografier og fingeraftryk og visummyndigheders tilknyttede afgørelser samt forbindelser mellem relaterede ansøgninger. VIS anvender et biometrisk system til at sikre pålidelige fingeraftrykssammenligninger med henblik på enten

- bekræftelse, dvs. kontrol af, om fingeraftryk, der scannes ved et grænseovergangssted, svarer til de fingeraftryk, der indgår i de biometriske data i det pågældende visum, eller

- identifikation, dvs. sammenligning af fingeraftryk, der tages ved et grænseovergangssted, med hele databasens indhold.

Teknisk set består VIS af tre niveauer, nemlig det centrale, det nationale og det lokale niveau, hvor sidstnævnte omfatter konsulære repræsentationer, grænseovergangssteder samt indvandrings- og politimyndigheder.
I maj 2018 forelagde Kommissionen et lovgivningsforslag om ændring af VIS-forordningen, der bl.a. tager sigte på at sikre interoperabilitet mellem andre databaser inden for retlige og indre anliggender. Det opgraderede VIS forventes ikke at være operationelt inden udgangen af 2021.

2.7. Eurodac[4950]

Det europæiske automatiske fingeraftryksidentifikationssystem (Eurodac) medvirkede oprindelig til at afgøre, hvilken medlemsstat der er ansvarlig for behandling af en asylansøgning, der indgives i en af medlemsstaterne, og i øvrigt til at lette anvendelsen af Dublinkonventionen. Adgang til Eurodac med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger gives kun i veldefinerede tilfælde.

Forordning (EU) nr. 603/2013 (Eurodacforordningen) fastsætter regler for videregivelse af fingeraftryksoplysninger til den centrale enhed, registrering af disse oplysninger og andre relevante oplysninger i den relevante centrale database, lagring af oplysningerne, sammenligning af oplysningerne med andre fingeraftryksoplysninger, videregivelse af resultaterne af denne sammenligning samt blokering og sletning af registrerede oplysninger.

Eurodacsystemets arkitektur består af a) en central elektronisk fingeraftryksdatabase ("det centrale system") bestående af en central enhed og en beredskabsplan og et beredskabssystem og b) en kommunikationsinfrastruktur mellem det centrale system og medlemsstaterne, der sikrer et krypteret virtuelt netværk forbeholdt Eurodacoplysninger ("kommunikationsinfrastrukturen").

Hver medlemsstat har ét nationalt adgangspunkt.

Eu-LISA, der er oprettet ved forordning (EU) nr. 1077/2011[51], har ansvaret for den operationelle forvaltning af Eurodac og sikrer i samarbejde med medlemsstaterne, at de bedste disponible og sikreste teknologier og teknikker, på grundlag af en cost-benefit-analyse, til enhver tid anvendes til det centrale system.

---

49 Rådets forordning (EF) nr. 2725/2000 af 11. december 2000 om oprettelse af "Eurodac" til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af Dublinkonventionen (EFT L 316 af 15.12.2000, s. 1).

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

51 Europa-Parlamentets og Rådets forordning (EU) nr. 1077/2011 af 25. oktober 2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store IT-systemer inden for området med frihed, sikkerhed og retfærdighed (EUT L 286 af 1.11.2011, s. 1).

Enhver medlemsstat kan videregive fingeraftryk til den centrale enhed med henblik på at kontrollere, om en udlænding, der er fyldt 14 år og opholder sig ulovligt på dens område, allerede har indgivet en asylansøgning i en anden medlemsstat. Den centrale enhed sammenligner disse fingeraftryk med fingeraftryksoplysninger, der er videregivet af andre medlemsstater, og som allerede er lagret i den centrale database. Enheden underretter den medlemsstat, der har videregivet oplysningerne, om der er et "hit", dvs. resultatet af sammenligningen af de registrerede og de videregivne fingeraftryk. Denne medlemsstat kontrollerer resultatet og foretager en endelig identifikation i samarbejde med de berørte medlemsstater.

Medlemsstaterne skal sikre Eurodacoplysningernes lovlighed, rigtighed og sikkerhed. Enhver person eller medlemsstat, som har lidt skade som følge af manglende overholdelse af Eurodacbestemmelserne, har ret til erstatning fra den medlemsstat, der er ansvarlig for skaden.

Forordning (EU) nr. 603/2013 indeholder bestemmelser om adgang til Eurodacoplysninger for medlemsstaternes udpegede myndigheder og Europol med henblik på retshåndhævelse. I henhold til forordningen kan udpegede myndigheder kun indgive en begrundet elektronisk anmodning om sammenligning af fingeraftryksoplysninger med de oplysninger, der er lagret i det centrale system, hvis sammenligning med følgende databaser ikke har ført til identifikation af den registrerede:

– nationale fingeraftryksdatabaser

– alle andre medlemsstaters elektroniske fingeraftryksidentifikationssystemer (AFIS) i henhold til Rådets afgørelse 2008/615/RIA ("Prümafgørelsen"), hvis sammenligninger er teknisk mulige, medmindre der er rimelig grund til at antage, at sammenligning med disse systemer ikke vil føre til identifikation af den registrerede. Sådanne rimelige grunde skal anføres i den begrundede elektroniske anmodning om sammenligning med Eurodacoplysninger, som den pågældende udpegede myndighed sender til kontrolmyndigheden

– visuminformationssystemet (VIS), forudsat at betingelserne for en sådan sammenligning i afgørelse 2008/633/RIA er opfyldt.

Følgende kumulative betingelser skal også være opfyldt:

a) Sammenligning er nødvendig med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger, hvilket betyder, at der foreligger et tungtvejende hensyn til den offentlige sikkerhed, der gør det forholdsmæssigt at søge i databasen.

b) Sammenligning er nødvendig i det specifikke tilfælde (dvs. at systematiske sammenligninger ikke må foretages).

c) Der er rimelig grund til at antage, at en sammenligning vil bidrage væsentligt til forebyggelse, afsløring eller efterforskning af den pågældende strafbare handling. Sådanne rimelige grunde foreligger navnlig, når der er begrundet mistanke om, at den person, der mistænkes for, har begået eller er offer for en terrorhandling eller en anden alvorlig strafbar handling, falder ind under en kategori, der er omfattet af forordning (EU) nr. 603/2013.

2.8. Toldinformationssystemet (CIS)[52]

Toldinformationssystemet supplerer Napoli II-konventionen[53]. Systemet tilsigter at styrke medlemsstaternes toldmyndigheder gennem hurtig udveksling af oplysninger med henblik på at forebygge, efterforske og retsforfølge alvorlige overtrædelser af national ret og EU-retten. Med CIS oprettes også et elektronisk sagsregister på toldområdet (FIDE) til bistand for toldefterforskninger.

CIS, der forvaltes af Kommissionen, er et centraliseret informationssystem, som er tilgængeligt via terminaler i medlemsstaterne og i Kommissionen, Europol og Eurojust. Nationale told-, skatte- og landbrugsmyndigheder og offentlige sundhedsmyndigheder og politimyndigheder samt Europol og Eurojust har adgang til CIS-oplysninger. Kun de myndigheder, der er udpeget af medlemsstaterne[54], og Kommissionen har direkte adgang til oplysningerne i CIS. For at øge komplementariteten har Europol og Eurojust læseadgang til CIS og FIDE.

---

52 Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet (EUT L 323 af 10.12.2009, s. 20).

53 Konvention, udarbejdet på grundlag af artikel K.3 i traktaten om Den Europæiske Union, om gensidig bistand og samarbejde mellem toldmyndighederne (EFT C 24 af 23.1.1998, s. 2).

54 Gennemførelse af artikel 7, stk. 2, og artikel 8, stk. 3, i Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet – ajourførte lister over kompetente myndigheder (13394/11 ENFOCUSTOM 85).

CIS omfatter personoplysninger i forbindelse med råvarer, transportmidler, virksomheder, personer, varer og likvide midler, der er tilbageholdt, beslaglagt eller konfiskeret. Personoplysninger må kun kopieres fra CIS til andre databehandlingssystemer med henblik på risikostyring eller operationelle analyser, som kun analytikere udpeget af medlemsstaterne må få adgang til.

FIDE giver de nationale myndigheder, der har ansvaret for at foretage toldefterforskning, mulighed for, når de åbner en efterforskningssag, at identificere andre myndigheder, der måtte have efterforsket en bestemt person eller virksomhed.

2.9. Falske og ægte dokumenter online (FADO)[55]

Dette elektroniske billedlagringssystem, der omfatter falske og ægte dokumenter og er baseret på internetteknologi, muliggør hurtig og sikker udveksling af oplysninger mellem Generalsekretariatet for Rådet for Den Europæiske Union og dokumentkontrollører i alle medlemsstaterne samt i Island, Norge og Schweiz. Systemet muliggør skærmsammenligning af originale og falske eller forfalskede dokumenter. Det indeholder først og fremmest dokumenter fra medlemsstaterne og dokumenter fra de tredjelande, hvorfra der er regelmæssige indvandringsstrømme til medlemsstaterne. Den database, der er oprettet i forbindelse med FADO, omfatter følgende oplysninger:

- billeder af ægte dokumenter
- oplysninger om sikkerhedsteknikker (sikkerhedsfeatures)
- billeder af typiske falske og forfalskede dokumenter
- oplysninger om forfalskningsteknikker og
- statistik over afslørede falske og forfalskede dokumenter og identitetssvig.

[55] Fælles aktion 98/700/RIA af 3. december 1998 vedtaget af Rådet på grundlag af artikel K.3 i traktaten om Den Europæiske Union om oprettelse af et europæisk system for lagring og overførsel af billeder (FADO) (EFT L 333 af 9.12.1998, s. 4).

Systemet anvender særlige datalinjer mellem Generalsekretariatet for Rådet og de centrale tjenester, der befinder sig i medlemsstaterne. I hver medlemsstat er der adgang til systemet via en sikker internetforbindelse fra en central tjeneste. En medlemsstat kan anvende systemet internt på sit eget område, hvilket indebærer, at forskellige arbejdsstationer på medlemsstatens forskellige grænsekontrolsteder eller hos andre kompetente myndigheder forbindes. Bortset fra den nationale centrale tjeneste er der dog ingen direkte forbindelse mellem en arbejdsstation og det centrale punkt i generalsekretariatet.

FADO er i øjeblikket tilgængeligt på 22 officielle EU-sprog. Dokumenter indlæses af dokumenteksperter på et af sprogene, og de standardiserede beskrivelser oversættes automatisk. Dokumenter er derfor straks tilgængelige på alle understøttede sprog. Supplerende fritekstoplysninger i de pågældende dokumenter oversættes derefter af specialiserede oversættere i Generalsekretariatet for Rådet.

2.10. Offentligt onlineregister over ægte identitetspapirer og rejselegitimation (PRADO)

Mens adgang til FADO er begrænset til dokumentkontrollører og myndigheder, indeholder Rådet for Den Europæiske Unions offentlige onlineregister over ægte identitetspapirer og rejselegitimation (PRADO) et uddrag af oplysningerne i FADO, der er tilgængeligt for offentligheden. Generalsekretariatet for Rådet for Den Europæiske Union stiller dette websted[56] til rådighed på de officielle EU-sprog af hensyn til gennemsigtigheden, og det er en vigtig tjeneste for mange brugere i Europa, især ikkestatslige organisationer med behov for eller en retlig forpligtelse til at kontrollere personers identitet.

Webstedet indeholder tekniske beskrivelser, herunder oplysninger om sikkerhedsfeatures, af ægte identitetspapirer og rejselegitimation. Oplysningerne udvælges og videregives af dokumenteksperter i medlemsstaterne samt Island, Norge og Schweiz.

I PRADO kan brugerne også finde link til websteder med oplysninger om ugyldige dokumentnumre fra visse medlemsstater samt tredjelande og andre nyttige oplysninger om identitets- og dokumentkontrol og identitetssvig og dokumentfalsk.

---

[56] http://www.prado.consilium.europa.eu/

2.11. Ind- og udrejsesystemet (EES)

Ind- og udrejsesystemet[57] (EES) sigter primært mod at forbedre forvaltningen af EU's ydre grænser[58]. Det registrerer elektronisk, hvor og hvornår visse tredjelandsstatsborgere, der har fået indrejse med henblik på et kortvarigt ophold på medlemsstaternes område, ind- og udrejser, og beregner varigheden af deres tilladte ophold.

Derudover kan de nationale retshåndhævende myndigheder kun søge i EES på de betingelser, der er fastsat i forordningen, med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger.

Forordningen fastsætter strenge regler for adgang til EES. Den indeholder også regler om enkeltpersoners ret til indsigt, berigtigelse, supplering, sletning og klageadgang, navnlig retten til domstolsprøvelse og uafhængige offentlige myndigheders tilsyn med behandlingen af oplysningerne. Forordningen overholder de grundlæggende rettigheder og de principper, der er fastlagt i EU's charter om grundlæggende rettigheder.

EES består af

- et centralt system (det centrale EES-system), som anvender en central elektronisk database med biometriske data (fingeraftryksoplysninger og ansigtsbilleder) og alfanumeriske data
- en national ensartet grænseflade i hver medlemsstat
- en sikker og krypteret kommunikationsinfrastruktur, der forbinder det centrale EES-system med den nationale ensartede grænseflade
- en sikker kommunikationskanal, som forbinder det centrale EES-system med visuminformationssystemet (VIS) med henblik på søgning.

---

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

58 Kommissionen bestemmer, fra hvilken dato EES skal idriftsættes, når betingelserne i artikel 66 i forordning (EU) 2017/2226 er opfyldt.

Forordningen præciserer, hvilke nationale myndigheder der kan få tilladelse til at få adgang til EES for at registrere, ændre, slette eller indhente oplysninger med henblik på EES' specifikke formål og i det omfang, det er nødvendigt, for at de kan udføre deres opgaver. Enhver behandling af oplysninger i EES bør stå i et rimeligt forhold til de forfulgte mål og være nødvendig for, at de kompetente myndigheder kan udføre deres opgave.

Betingelserne for at give de nationale retshåndhævende myndigheder adgang til EES er af en sådan art, at de kan gøre det muligt for disse myndigheder at tage fat på sager, hvor mistænkte anvender flere identiteter. Specifik brug af biometriske data, der er lagret i EES, er berettiget, skønt det har en indvirkning på den rejsendes privatliv, for at identificere rejsende uden rejsedokumentation eller anden identifikation. Sådanne data kan dog også bruges som et efterforskningsværktøj til at tilvejebringe beviser ved at spore rejseruter for en person, der mistænkes for at have begået en forbrydelse, eller et offer for en forbrydelse.

Adgang til EES-oplysninger til retshåndhævelsesformål udgør et indgreb i den grundlæggende ret til respekt for privatliv og beskyttelse af personoplysninger for personer, hvis oplysninger behandles i EES. Denne behandling er underlagt bestemmelserne i direktiv (EU) 2016/680 ("politidirektivet")[59].

De nationale retshåndhævende myndigheder kan ved udførelsen af deres opgaver sammenligne et fingeraftryksspor, der er fundet på et gerningssted ("latente fingeraftryk"), med fingeraftryksoplysninger, der er lagret i EES, hvis der er rimelig grund til at antage, at gerningsmanden eller offeret er lagret i EES. Retshåndhævende myndigheders adgang til EES for at identificere ukendte mistænkte, gerningsmænd eller ofre for terrorhandlinger eller andre grove strafbare handlinger er imidlertid betinget af, at der er foretaget søgninger i de nationale databaser, og at fingeraftrykssøgningen i henhold til Rådets afgørelse 2008/615/RIA[60] ("Prümafgørelsen") er blevet gennemført fuldt ud, eller at søgningen ikke er blevet gennemført fuldt ud inden for to dage efter dens iværksættelse.

---

[59] Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2019 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).

[60] Rådets afgørelse 2008/615/RIA af 23. juni 2008 om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (EUT L 210 af 6.5.2008, s. 1).

I lighed med procedurerne og betingelserne for de nationale retshåndhævende myndigheders adgang er oplysninger fra EES også tilgængelige for Europol inden for rammerne af dets opgaver og med forbehold af de betingelser og begrænsninger, der er fastsat i forordningen. Europol behandler oplysninger modtaget ved søgning i EES efter tilladelse fra oprindelsesmedlemsstaterne. Denne tilladelse indhentes via Europols nationale enhed i den pågældende medlemsstat. Den Europæiske Tilsynsførende for Databeskyttelse bør føre tilsyn med Europols behandling af personoplysninger og sikre fuld overholdelse af gældende databeskyttelsesregler.

2.12. EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS)[61]

Udveksling af oplysninger om grænseforvaltning, retshåndhævelse og bekæmpelse af terrorisme vil blive støttet af ETIAS[62]. Systemet har til formål at fastlægge, hvorvidt tredjelandsstatsborgere, der er fritaget for visumpligt, opfylder betingelserne herfor, inden de rejser til Schengenområdet og forud for deres ankomst til grænseovergangssteder ved de ydre grænser. ETIAS giver en rejsetilladelse, der i sig selv er forskellig fra et visum, men som udgør en betingelse for indrejse og ophold, og som viser, at ansøgeren ikke udgør en risiko for sikkerheden, en risiko for ulovlig indvandring eller en høj risiko for epidemi. Udstedte rejsetilladelser bør annulleres eller inddrages, så snart det bliver åbenlyst, at betingelserne for at udstede dem ikke var eller ikke længere er opfyldt.

ETIAS består af et:

- omfattende informationssystem, dvs. ETIAS-informationssystemet, der er udformet, udviklet og teknisk forvaltet af eu-LISA
- Den centrale ETIAS-enhed, som er del af Det Europæiske Agentur for Grænse- og Kystbevogtning

---

61 Europa-Parlamentets og Rådets forordning (EU) 2018/1240 af af 12. september 2018 om oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) og om ændring af forordning (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399 (EU) 2016/1624 og (EU) 2017/2226 (EUT L 236 af 19.9.2018, s. 1).
Europa-Parlamentets og Rådets forordning (EU) 2018/1241 af 12. september 2018 om ændring af forordning (EU) 2016/794 med henblik på oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) (EUT L 236 af 19.9.2018, s. 72).

62 Kommissionen bestemmer, fra hvilken dato EES skal idriftsættes, når betingelserne i artikel 88 i forordning (EU) 2018/1240 er opfyldt.

- De nationale ETIAS-enheder, ansvarlige for at behandle ansøgninger og afgøre, om de vil udstede eller afvise, annullere eller inddrage rejsetilladelser. Med henblik herpå bør de nationale enheder samarbejde med hinanden og med Europol med henblik på at vurdere ansøgninger.

Personoplysningerne fra ansøgeren behandles udelukkende af ETIAS med henblik på at vurdere, om ansøgerens indrejse i Unionen kan udgøre en trussel for sikkerheden i eller ulovlig indvandring til eller en høj risiko for epidemi i Unionen. Med henblik på risikovurderingen bør de angivne personoplysninger sammenlignes med oplysningerne i et register, en mappe eller en indberetning i et EU-informationssystem eller en EU-database (det centrale ETIAS-system, SIS, visuminformationssystemet (VIS), ind- og udrejsesystemet (EES) eller Eurodac), med Europoloplysningerne eller INTERPOL's databaser (INTERPOL's database over stjålne og bortkomne rejsedokumenter (SLTD) eller INTERPOL's database over rejsedokumenter med tilknyttede notifikationer (TDAWN). Personoplysningerne bør også sammenlignes med ETIAS-overvågningslisten og med specifikke risikoindikatorer.

Sammenligningen foregår automatisk. Hvis der forekommer et "hit", dvs. en overensstemmelse mellem personoplysninger i ansøgningen og de specifikke risikoindikatorer eller personoplysningerne i enten et register eller en indberetning i ovennævnte informationssystemer eller overvågningslisten, bør ansøgningen behandles manuelt af den ansvarlige medlemsstats nationale enhed. En sådan vurdering bør føre til, at der træffes afgørelse om at udstede rejsetilladelsen eller ej.

For at nå de overordnede mål for ETIAS skal betydelige mængder personoplysninger behandles. Forordningen respekterer de grundlæggende rettigheder og overholder de principper, der er anerkendt i Den Europæiske Unions charter om grundlæggende rettigheder. De fornødne garantier har derfor til formål at begrænse indgrebet i retten til beskyttelse af privatlivets fred og retten til beskyttelse af personoplysninger til, hvad der er nødvendigt og rimeligt i et demokratisk samfund. Af samme grund bør de kriterier, der anvendes til at definere de specifikke risikoindikatorer, under ingen omstændigheder baseres på følsomme personoplysninger[63].

---

[63] Jf. 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 (EUT L 119 af 4.5.2016, s. 1).

Adgangen til personoplysninger i ETIAS bør være forbeholdt direkte bemyndiget personale, og adgangen bør under ingen omstændigheder anvendes til at træffe afgørelser baseret på nogen form for forskelsbehandling. Hvad angår de retshåndhævende myndigheder, bør behandlingen af personoplysninger lagret i det centrale ETIAS-system kun finde sted i særlige tilfælde og kun, når det er nødvendigt med henblik på at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger. De udpegede myndigheder og Europol bør kun anmode om adgang til ETIAS, når de med rimelighed kan antage, at en sådan adgang vil kunne tilvejebringe oplysninger, der kan hjælpe dem med at forebygge, afsløre eller efterforske en terrorhandling eller en anden alvorlig strafbar handling.

2.13. Sammenfattende oversigt over informationssystemer, der anvendes til udveksling af oplysninger i EU

IT-systemer og databaser	Retsgrundlag	Formål	Registrerede	Datadeling
Anden generation af Schengeninformationssystemet **SIS II**	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)	• Indre sikkerhed • Grænsekontrol • Retligt samarbejde • Efterforskning af kriminalitet	• EU-borgere • Tredjelandsstatsborgere	• VIS • Europol • Eurojust • INTERPOL
	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 23.12.2006, s. 4)	• Nægtelse af indrejse eller ophold • Asyl-, indvandrings- og tilbagesendelsespolitikker	• Tredjelandsstatsborgere, der ikke har ret til fri bevægelighed svarende til EU-borgeres ret	
Europol **Europols informationssystem (EIS)**	Rådets afgørelse 2009/371/RIA af 6. april 2009 om oprettelse af Den Europæiske Politienhed (Europol), artikel 11-13 (EUT L 121 af 15.5.2009, s. 37)	• Grov kriminalitet • Indvandring • Indre sikkerhed • Terrorbekæmpelse	• EU-borgere • Tredjelandsstatsborgere	• SIS II
INTERPOL **I-24/7**	Statutterne for INTERPOL		• EU-borgere • Tredjelandsstatsborgere	• SIS II • Europol • VIS

INTERPOL **Stjålne og bortkomne rejsedokumenter (SLTD)**	Rådets fælles holdning 2005/69/RIA af 24. januar 2005 om udveksling af bestemte oplysninger med INTERPOL (EUT L 27 af 29.1.2005, s. 61)	• International og organiseret kriminalitet • Indre sikkerhed	• EU-borgere • Tredjelandsstatsborgere	
Det europæiske informationssystem vedrørende strafferegistre (ECRIS)	Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 171 af 7.6.2019, s. 143)	Straffesager	• EU-borgere • Tredjelandsstatsborgere	
ECRIS-TCN	Europa-Parlamentets og Rådets forordning (EU) 2019/816 af 17. april 2019 om oprettelse af et centralt system til bestemmelse af, hvilke medlemsstater der ligger inde med oplysninger om straffedomme afsagt over tredjelandsstatsborgere og statsløse personer (ECRIS-TCN) for at supplere det europæiske informationssystem vedrørende strafferegistre, og om ændring af forordning (EU) 2018/1726 (EUT L 135 af 22.5.2019, s. 1) Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 171 af 7.6.2019, s. 143)	Straffesager	• Tredjelandsstatsborgere	• Europol • Eurojust • EPPO

VIS	Rådets beslutning 2004/512/EF af 8. juni 2004 om indførelse af visuminformationssystemet (VIS) (EUT L 213 af 15.6.2004, s. 5) Rådets afgørelse 2008/633/RIA af 23. juni 2008 om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (EUT L 218 af 13.8.2008, s. 129) Rådets afgørelse 2013/392/EU af 22. juli 2013 om fastsættelse af den dato, fra hvilken afgørelse 2008/633/RIA om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger har virkning (EUT L 198 af 23.7.2013, s. 45)	• Grov kriminalitet • Indre sikkerhed • Terrorbekæmpelse	• Tredjelandsstatsborgere	• SIS II • Europol • INTERPOL

Eurodac	Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 af 26. juni 2013 om oprettelse af "Eurodac" til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet i en af medlemsstaterne af en tredjelandsstatsborger eller en statsløs, og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse og om ændring af forordning (EU) nr. 1077/2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store IT-systemer inden for området med frihed, sikkerhed og retfærdighed (omarbejdning) (EUT L 180 af 29.6.2013, s. 1) Europa-Parlamentets og Rådets forordning (EU) nr. 604/2013 af 26. juni 2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelandsstatsborger eller en statsløs i en af medlemsstaterne (EUT L 180 af 29.6.2013, s. 31)	• Indvandring • Grov kriminalitet • Indre sikkerhed • Terrorbekæmpelse	• Tredjelandsstatsborgere	Europol

Passagerlister **(PNR)**	Europa-Parlamentets og Rådets direktiv (EU) 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (EUT L 119 af 4.5.2016, s. 132)	• Grov kriminalitet • Indre sikkerhed • Terrorbekæmpelse	• EU-borgere • Tredjelandsstatsborgere	Europol
Forhåndsinformation om passagerer (API)	Rådets direktiv 2004/82/EF af 29. april 2004 om transportvirksomheders forpligtelse til at fremsende oplysninger om passagerer (EUT L 261 af 6.8.2004, s. 24)	• Grænsekontrol • Indvandring	• Tredjelandsstatsborgere	
ETIAS	Europa-Parlamentets og Rådets forordning (EU) 2018/1240 af 12. september 2018 om oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) og om ændring af forordning (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 og (EU) 2017/2226[64] (EUT L 236 af 19.9.2018, s. 1) Europa-Parlamentets og Rådets forordning (EU) 2018/1241 af 12. september 2018 om ændring af forordning (EU) 2016/794 med henblik på oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) (EUT L 236 af 19.9.2018, s. 72)	• Grænsekontrol • Indvandring • Grov kriminalitet • Indre sikkerhed • Terrorbekæmpelse	• Tredjelandsstatsborgere	• SIS • VIS • EES • Eurodac • Europol • INTERPOL • ETIAS-overvågningsliste

[64] Kommissionen bestemmer, fra hvilket tidspunkt ETIAS skal idriftsættes, når betingelserne i artikel 88 i forordningen er opfyldt.

EES	Europa-Parlamentets og Rådets forordning (EU) 2017/2225 af 30. november 2017 om ændring af forordning (EU) 2016/399, for så vidt angår brugen af ind- og udrejsesystemet (EUT L 327 af 9.12.2017, s. 1) Europa-Parlamentets og Rådets forordning (EU) 2017/2226 af 30. november 2017 om oprettelse af et ind- og udrejsesystem til registrering af ind- og udrejseoplysninger og oplysninger om nægtelse af indrejse vedrørende tredjelandsstatsborgere, der passerer medlemsstaternes ydre grænser, om fastlæggelse af betingelserne for adgang til ind- og udrejsesystemet til retshåndhævelsesformål og om ændring af konventionen om gennemførelse af Schengenaftalen og forordning (EF) nr. 767/2008 og (EU) nr. 1077/2011[65] (EUT L 327 af 9.12.2017, s. 20)	• Grænseforvaltning • Grov kriminalitet • Terrorbekæmpelse	• Tredjelandsstatsborgere	• VIS • Europol • Prümafgørelsen
SNG	Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet (EUT L 323 af 10.12.2009, s. 20)	• Bekæmpelse af ulovlig handel	• Europæiske borgere • Tredjelandsstatsborgere	Europol

[65] Kommissionen bestemmer, fra hvilket tidspunkt EES skal idriftsættes, når betingelserne i artikel 66 i forordningen er opfyldt.

FADO	Fælles aktion 98/700/RIA af 3. december 1998 vedtaget af Rådet på grundlag af artikel K.3 i traktaten om Den Europæiske Union om oprettelse af et europæisk system for lagring og overførsel af billeder (FADO) (EFT L 333 af 9.12.1998, s. 4)	• Bekæmpelse af falske dokumenter • Indvandringspolitik • Politisamarbejde	• Europæiske borgere • Tredjelandsstatsborgere	

3. LOVGIVNING – RETLIG RAMME, REGLER OG RETNINGSLINJER FOR DE VIGTIGSTE KOMMUNIKATIONSMETODER OG - SYSTEMER

3.1. Databeskyttelsesdirektivet[66]

Direktiv (EU) 2016/680, der ophæver Rådets rammeafgørelse 2008/977/RIA[67], fastsætter særlige bestemmelser for

- beskyttelse af fysiske personer uanset nationalitet eller bopæl i forbindelse med behandling af personoplysninger, enten ved hjælp af elektronisk databehandling eller på anden måde, af politiet eller andre retshåndhævende myndigheder inden for rammerne af deres aktiviteter og

- de kompetente myndigheders udveksling af personoplysninger inden for Unionen med henblik på at forebygge, efterforske, opdage eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner.

Dette har til formål at sikre det samme beskyttelsesniveau for fysiske personer ved hjælp af rettigheder, der kan håndhæves retsligt i hele Unionen, og forhindre forskellig praksis, der hæmmer udvekslingen af personoplysninger mellem de kompetente myndigheder.

Medlemsstaterne skal gennemføre direktivet i national ret senest den 6. maj 2018. I tilfælde, hvor dette indebærer en uforholdsmæssig stor indsats, kan de dog undtagelsesvis bestemme, at de senest den 6. maj 2023 vil gennemføre de relevante bestemmelser om overvågning af operationer i elektroniske databehandlingssystemer, der er oprettet før den 6. maj 2016.

---

66 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).

67 Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (EUT L 350 af 30.12.2008, s. 60). Rammeafgørelsen ophæves med virkning fra den 6. maj 2018.

Udtrykket "kompetente myndigheder" omfatter offentlige myndigheder som judicielle myndigheder, politi eller andre retshåndhævende myndigheder samt alle andre organer eller enheder, som i henhold til en medlemsstats ret udøver offentlig myndighed eller offentlige beføjelser med henblik på dette direktiv. De retshåndhævende myndigheders aktiviteter fokuserer hovedsageligt på forebyggelse, efterforskning, opdagelse eller retsforfølgelse af straffelovsovertrædelser. Sådanne aktiviteter kan også omfatte politiaktiviteter ved demonstrationer, store sportsbegivenheder og uroligheder. De omfatter også opretholdelse af lov og orden som en opgave, der er overdraget til dem, når det er nødvendigt, for at beskytte mod og forebygge trusler mod den offentlige sikkerhed og de grundlæggende interesser i samfundet, som kan føre til en straffelovsovertrædelse.

Behandling af personoplysninger, der sker til formål uden for rammerne af ovennævnte aktiviteter, og som medlemsstaterne desuden kan overdrage til de retshåndhævende myndigheder, samt behandling af personoplysninger, for så vidt som dette er omfattet af EU-retten, er reguleret ved forordning (EU) nr. 2016/679[68]. Endvidere omfatter direktiv (EU) 2016/680 ikke behandling af personoplysninger med hensyn til aktiviteter vedrørende national sikkerhed, aktiviteter gennemført af agenturer eller enheder, der beskæftiger sig med nationale sikkerhedsspørgsmål, eller behandling af personoplysninger, der foretages af medlemsstaterne, når de gennemfører aktiviteter vedrørende den fælles udenrigs- og sikkerhedspolitik[69].

Med henblik på anvendelsen af databeskyttelsesdirektivet forstås ved:

- **"personoplysninger"**: enhver form for information om en fysisk person ("den registrerede"), der er identificeret, eller som kan identificeres direkte eller indirekte, især ved henvisning til et navn, et identifikationsnummer, lokaliseringsdata, onlineidentifikation eller en eller flere faktorer, der er specifikke for den pågældende fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

  Medlemsstaterne fastsætter, at de kompetente myndigheder, der behandler personoplysninger, hvis det er relevant og i videst muligt omfang, skal sondre klart mellem personoplysninger om forskellige kategorier af registrerede såsom a) mistænkte, b) domfældte, c) ofre og d) andre parter i en kriminel handling som f.eks. vidner.

---

68 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).

69 Afsnit V, kapitel 2, i traktaten om Den Europæiske Union (TEU).

- **"behandling"**: enhver aktivitet eller række af aktiviteter med eller uden brug af automatisk behandling, som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

Personoplysninger skal behandles lovligt og rimeligt og kun til specifikke formål fastlagt ved lov. For at være lovlig bør en sådan behandling være nødvendig for at løse en opgave, der udføres af en kompetent myndighed med henblik på ovennævnte retshåndhævelse. Databeskyttelsesprincippet om rimelig behandling er et særskilt begreb i forhold til retten til en retfærdig rettergang som defineret i chartrets artikel 47 og artikel 6 i konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (EMRK). Personoplysningerne skal være tilstrækkelige og relevante i forhold til de formål, hvortil de behandles.

Behandling af særligt følsomme personoplysninger om race eller etnisk oprindelse, politiske anskuelser, religiøs eller filosofisk overbevisning eller medlemskab af en fagforening og behandling af genetiske data, biometriske data alene med henblik på at identificere en fysisk person, helbredsoplysninger eller oplysninger vedrørende en fysisk persons seksualitet eller seksuelle orientering er kun tilladt, når det er strengt nødvendigt, med forbehold af de fornødne garantier for den registreredes rettigheder og frihedsrettigheder, og kun på nøje fastlagte og restriktive betingelser.

Oprettelsen af nationale tilsynsmyndigheder, som kan udøve deres hverv i fuld uafhængighed, har afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af oplysninger om dem. Tilsynsmyndighederne bør overvåge anvendelsen af de bestemmelser, der vedtages i medfør af dette direktiv, og bidrage til en ensartet anvendelse heraf i hele Unionen. Beskyttelsen af registreredes rettigheder og frihedsrettigheder samt de nationale kompetente myndigheders og databehandleres ansvar og forpligtelser, bl.a. i forbindelse med tilsynsmyndighedernes overvågning og foranstaltninger truffet af disse myndigheder, kræver en klar ansvarstildeling.

Flytning af personlige oplysninger på tværs af grænserne kan bringe fysiske personers evne til at beskytte sig selv juridisk mod ulovlig brug eller videregivelse af disse oplysninger i fare. Samtidig må tilsynsmyndighederne i nogle tilfælde konstatere, at de ikke kan følge op på klager eller gennemføre undersøgelser vedrørende aktiviteter uden for deres grænser. Samarbejdet på tværs af grænserne kan også hæmmes af utilstrækkelige forebyggende eller afhjælpende beføjelser og uensartede retlige ordninger. Der er derfor behov for at fremme et tættere samarbejde mellem tilsynsmyndighederne for databeskyttelse for at lette udvekslingen af oplysninger med tilsvarende udenlandske myndigheder.

3.2. "Den svenske rammeafgørelse" (SFD)[70]

Som videreudvikling af Schengenreglerne fastsætter Rådets rammeafgørelse 2006/960/RIA ("den svenske rammeafgørelse" (SFD)) navnlig regler vedrørende tidsfrister og standardformularer til grænseoverskridende udveksling af oplysninger[71], efter anmodning eller uanmodet, mellem de udpegede kompetente retshåndhævende myndigheder i medlemsstaterne med henblik på:

- at forebygge, afsløre og efterforske lovovertrædelser eller kriminelle aktiviteter, som kan sidestilles med eller svarer til dem, der er omhandlet i den europæiske arrestordre[72], eller
- at forebygge en umiddelbar og alvorlig trussel mod den offentlige sikkerhed.

De udpegede myndigheder skal svare inden for højst otte timer i hastetilfælde, så længe de ønskede oplysninger eller efterretninger er direkte tilgængelige for de retshåndhævende myndigheder. Oplysninger må ikke gives, hvis:

- den nationale sikkerhed er på spil
- igangværende efterforskninger kan bringes i fare

---

70 Rådets rammeafgørelse 2006/960/RIA af 18. december 2006 om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder (EUT L 386 af 29.12.2006, s. 89, med berigtigelse i EUT L 75 af 15.3.2007, s. 26).

71 Jf. figur 1 nedenfor.

72 Den endelige udgave af den europæiske håndbog om udstedelse af en europæisk arrestordre (8216/2/08 REV 2). Artikel 2 i Rådets rammeafgørelse 2002/584/RIA om den europæiske arrestordre fastsætter anvendelsesområdet for den europæiske arrestordre.

- anmodningen vedrører en lovovertrædelse, der kan straffes med op til et års fængsel i henhold til den anmodede medlemsstats ret
- den kompetente judicielle myndighed nægter at give adgang til de pågældende oplysninger.

Betegnelserne "oplysninger og/eller efterretninger" omfatter følgende to kategorier:

– enhver form for oplysninger eller data, som de retshåndhævende myndigheder er i besiddelse af

– enhver form for oplysninger eller data, som offentlige myndigheder eller private foretagender er i besiddelse af, og som de retshåndhævende myndigheder har adgang til, uden at der foretages tvangsindgreb.

Indholdet af disse kategorier afhænger af national lovgivning. Typen af tilgængelige oplysninger fra hver medlemsstat er anført i de nationale faktablade, der er vedlagt denne håndbog.

Data skal deles med Europol, for så vidt som de udvekslede oplysninger eller efterretninger vedrører en lovovertrædelse eller kriminel aktivitet, der ligger inden for Europols mandat. Oplysninger og efterretninger behandles i overensstemmelse med Europols relevante håndteringskoder. SIENA (Europols netværksprogram til sikker informationsudveksling) understøtter udveksling af oplysninger i overensstemmelse med "den svenske rammeafgørelse".

Medlemsstaterne sikrer, at betingelserne for grænseoverskridende udveksling af oplysninger ikke er strengere end dem, der gælder for interne sager. De kompetente retshåndhævende myndigheder er navnlig ikke forpligtet til at anmode om godkendelse eller tilladelse fra en judiciel myndighed forud for grænseoverskridende udveksling af oplysninger, hvis de ønskede oplysninger er tilgængelige på nationalt plan uden en sådan godkendelse eller tilladelse. Hvis der imidlertid kræves tilladelse fra en judiciel myndighed, skal den judicielle myndighed anvende samme regler i forbindelse med sin afgørelse i en grænseoverskridende sag som i en rent intern sag. Oplysninger, der kræver tilladelse fra en judiciel myndighed, er angivet i de nationale faktablade.

Eftersom brugere har fundet standardanmodningsformularen for besværlig, er der blevet udarbejdet en ikkeobligatorisk formular til anmodninger om oplysninger og efterretninger[73]. Når det ikke er muligt at benytte denne forenklede formular, foretrækkes det, at en anden formular eller ustruktureret fritekst anvendes.

[73] Jf. figur 2 nedenfor.

Anmodninger skal dog i alle tilfælde opfylde kravene i artikel 5 i den svenske rammeafgørelse og mindst indeholde følgende obligatoriske elementer:

- administrative oplysninger, dvs. anmodende medlemsstat, anmodende myndighed, dato, referencenummer eller - numre samt den eller de anmodede medlemsstater
- om der er anmodet om hastebehandling, og i bekræftende fald hvorfor
- beskrivelse af de ønskede oplysninger eller efterretninger
- identitet (for så vidt den er kendt) af den eller de personer eller genstande, der er hovedemne(r) i den kriminalefterforskning eller kriminalefterretningsoperation, der ligger til grund for anmodningen om oplysninger eller efterretninger (f.eks. beskrivelse af lovovertrædelsen eller lovovertrædelserne, de omstændigheder, som lovovertrædelsen eller lovovertrædelserne blev begået under, osv.)
- formål med anmodningen om oplysninger eller efterretninger
- forbindelse mellem formålet og den person, som oplysningerne eller efterretningerne vedrører
- forhold, der giver anledning til at tro, at oplysningerne eller efterretningerne findes i den anmodede medlemsstat
- eventuelle begrænsninger for anvendelse af oplysningerne i anmodningen ("håndteringskoder").

Den anmodende medlemsstat kan vælge mellem de eksisterende kanaler for international retshåndhævelseskommunikation (SIRENE, Europol, INTERPOL eller bilaterale kontaktpunkter). Den svarende medlemsstat benytter normalt den samme kanal som den, der blev anvendt til anmodningen. Hvis den anmodede medlemsstat imidlertid af legitime grunde svarer via en anden kanal, underrettes den anmodende myndighed om denne ændring. Det sprog, der anvendes ved anmodning om og levering af oplysninger, skal være det, der gælder for den benyttede kanal.

En oversigt over **bilaterale aftaler og andre aftaler, der opretholdes**, er knyttet som bilag til denne håndbog.

Figur 1

BILAG A

UDVEKSLING AF OPLYSNINGER I HENHOLD TIL RÅDETS RAMMEAFGØRELSE 2006/960/RIA FORMULAR, DER SKAL ANVENDES AF DEN ANMODEDE MEDLEMSSTAT I TILFÆLDE AF VIDEREGIVELSE/FORSINKELSE AF VIDEREGIVELSE/AFVISNING AF VIDEREGIVELSE AF OPLYSNINGER

Denne formular anvendes til at videregive de ønskede oplysninger og/eller efterretninger, at underrette den anmodende myndighed om, at det er umuligt at overholde den normale tidsfrist, at anmodningen kræver tilladelse fra en judiciel myndighed, eller at videregivelse af oplysningerne afvises.

Formularen kan anvendes flere gange i løbet af proceduren (f.eks. hvis anmodningen først skal forelægges en judiciel myndighed, og det senere viser sig, at udførelsen af anmodningen må afslås).

Den anmodede myndighed (navn, adresse, tlf., fax, e-mail, medlemsstat)	
Oplysninger om speditør (fakultativt)	
Dette svars referencenummer	
Dato og referencenummer for tidligere svar	
Svar rettet til følgende anmodende myndighed	
Dato og klokkeslæt for anmodningen	
Anmodningens referencenummer	

Den normale tidsfrist i henhold til artikel 4 i rammeafgørelse 2006/960/RIA		
Lovovertrædelsen falder ind under artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA, og de ønskede oplysninger eller efterretninger er lagret i en database, som en retshåndhævende myndighed i den anmodede medlemsstat har direkte adgang til	Der blev anmodet om hastebehandling	→ ❑ 8 timer
	Der blev ikke anmodet om hastebehandling	→ ❑ 1 uge
Øvrige tilfælde		→ ❑ 14 dage

Oplysninger som videregives efter rammeafgørelse 2006/960/ria: de videregivne oplysninger og efterretninger
1. Anvendelse af videregivne oplysninger og efterretninger ❑ må kun anvendes til de formål, hvortil de er meddelt, eller til at forebygge en umiddelbar og alvorlig trussel mod den offentlige sikkerhed ❑ kan også anvendes til andre formål på følgende betingelser (fakultativt):
2. Kildens pålidelighed ❑ Pålidelig ❑ Stort set pålidelig ❑ Ikke pålidelig ❑ Kan ikke vurderes
3. Oplysningernes og efterretningernes nøjagtighed ❑ Sikre ❑ Angivet af kilden ❑ Bekræftet rygte ❑ Ubekræftet rygte

4. Resultatet af den kriminalefterforskning eller kriminalefterretningsoperation, inden for hvis rammer der er udvekslet oplysninger, skal meddeles den videregivende myndighed

❑ Nej
❑ Ja

5. Ved spontan udveksling af oplysninger: årsager til at antage, at oplysningerne eller efterretningerne kan bidrage til afsløring, forebyggelse eller efterforskning af lovovertrædelser som omhandlet i artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA:

FORSINKELSE - Det er ikke muligt at svare inden for den tidsfrist, der er fastsat i artikel 4 i rammeafgørelse 2006/960/RIA

Oplysningerne eller efterretningerne kan ikke gives inden for den givne tidsfrist af følgende årsager:

De vil formodentlig kunne gives i løbet af:

❑ 1 dag ❑ 2 dage ❑ 3 dage

❑ ... uger

❑ 1 måned

❑ Der er anmodet om tilladelse fra en judiciel myndighed
Der forventes at foreligge svar (imødekommelse/afslag) på anmodningen inden for ... uger

AFSLAG — Oplysningerne eller efterretningerne:

❑ kunne ikke videregives, og der kunne ikke anmodes om dem på nationalt plan, eller

❑ de kan ikke videregives af følgende grund(e):

A — Begrundelser baseret på judiciel kontrol, som er til hinder for videregivelse eller kræver anvendelse af gensidig retshjælp

❑ Den kompetente judicielle myndighed har ikke tilladt adgang til og udveksling af oplysningerne eller efterretningerne

❑ De ønskede oplysninger eller efterretninger er tidligere fremskaffet ved anvendelse af tvangsindgreb, og den nationale lovgivning åbner ikke mulighed for videregivelse

❑ Oplysningerne eller efterretningerne

- er ikke i de retshåndhævende myndigheders besiddelse, eller
- er ikke i offentlige myndigheders eller private foretagenders besiddelse på en måde, som giver de retshåndhævende myndigheder adgang til dem, uden at der foretages tvangsindgreb

❑ B — Videregivelse af de ønskede oplysninger eller efterretninger vil kunne skade vigtige nationale sikkerhedsinteresser eller vil kunne bringe et positivt udfald af en igangværende efterforskning, en kriminalefterretningsoperation eller enkeltpersoners sikkerhed i fare eller vil stå i klart misforhold til eller være irrelevant for det angivne formål

Hvis rubrik A eller B afkrydses, bedes De, hvis det skønnes nødvendigt anføre yderligere oplysninger eller begrunde afslaget (fakultativt):

❑ D — Den anmodede myndighed beslutter at afvise at imødekomme anmodningen, fordi den i henhold til den anmodede medlemsstats lovgivning vedrører følgende lovovertrædelse (lovovertrædelsens art og dens retlige kvalifikation angives) ....., der straffes med op til ét års fængsel

❑ E — De ønskede oplysninger eller efterretninger foreligger ikke

❑ F — De ønskede oplysninger eller efterretninger er fremskaffet hos en anden medlemsstat eller et tredjeland og er omfattet af specialitetsreglen, og den pågældende medlemsstat eller tredjeland har ikke givet sit samtykke til videregivelse af oplysningerne eller efterretningerne.

BILAG B

UDVEKSLING AF OPLYSNINGER I HENHOLD TIL RÅDETS RAMMEAFGØRELSE 2006/960/RIA FORMULAR TIL ANMODNING OM OPLYSNINGER OG EFTERRETNINGER, DER SKAL ANVENDES AF DEN ANMODENDE MEDLEMSSTAT

Denne formular anvendes, når der anmodes om oplysninger og efterretninger i henhold til rammeafgørelse 2006/960/RIA.

I — Administrative oplysninger

Den anmodende myndighed (navn, adresse, tlf., fax, e-mail, medlemsstat)	
Oplysninger om speditør (fakultativt)	
Rettet til følgende medlemsstat	
Dato og klokkeslæt for denne anmodning	
Anmodningens referencenummer	

Tidligere anmodninger				
❑ Dette er den første anmodning i denne sag				
❑ Denne anmodning følger efter tidligere anmodninger i samme sag				
Tidligere anmodning(er)			Svar	
	Dato	Referencenummer (i den anmodende medlemsstat)	Dato	Referencenummer (i den anmodede medlemsstat)
1.				
2.				
3.				
4.				

Hvis anmodningen sendes til mere end én myndighed i den anmodede medlemsstat, angives hver af de benyttede kanaler:	
❑ Den nationale enhed/Europol-forbindelsesofficer	❑ til orientering ❑ til imødekommelse
❑ Interpol-NCB	❑ til orientering ❑ til imødekommelse
❑ Sirene	❑ til orientering ❑ til imødekommelse
❑ Forbindelsesofficer	❑ til orientering ❑ til imødekommelse
❑ Andet (præciseres):	❑ til orientering ❑ til imødekommelse
Hvis den samme anmodning sendes til andre medlemsstater, angives de andre medlemsstater og de benyttede kanaler (fakultativt)	

II — Tidsfrister

Påmindelse: tidsfrister i henhold til artikel 4 i rammeafgørelse 2006/960/RIA

A — Lovovertrædelsen falder ind under artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA,

og

de ønskede oplysninger eller efterretninger er lagret i en database, som en retshåndhævende myndighed har direkte adgang til

→ Anmodningen haster → Tidsfrist: 8 timer med mulighed for udsættelse

→ Anmodningen haster ikke → Tidsfrist: 1 uge

B — Øvrige tilfælde: tidsfrist: 14 dage

❑ **Der ANMODES om hastebehandling**
❑ **Der ANMODES IKKE om hastebehandling**
Grunde til hastebehandling (f.eks. at mistænkte er varetægtsfængslet, eller at sagen skal for retten inden en bestemt dato):
De ønskede oplysninger eller efterretninger

Type kriminalitet eller kriminel(le) aktivitet(er), der efterforskes
Beskrivelse af de omstændigheder, under hvilke lovovertrædelsen eller lovovertrædelserne er begået, herunder tid og sted, og i hvilket omfang den person, der er genstand for oplysningerne eller efterretningerne, har deltaget i lovovertrædelsen eller lovovertrædelserne:

Lovovertrædelsens/lovovertrædelsernes karakter

A — Anvendelse af artikel 4, stk. 1 og 3, i rammeafgørelse 2006/960/RIA

❑ A.1. Lovovertrædelsen straffes med en fængselsstraf af en maksimal varighed på mindst tre år i den anmodende medlemsstat
OG
A.2. Det drejer sig om en (eller flere) af følgende lovovertrædelser:

- ❑ deltagelse i en kriminel organisation
- ❑ terrorisme
- ❑ menneskehandel
- ❑ seksuel udnyttelse af børn og børnepornografi
- ❑ ulovlig handel med narkotika og psykotrope stoffer
- ❑ ulovlig handel med våben, ammunition og eksplosive stoffer
- ❑ bestikkelse
- ❑ svig, herunder svig, der skader De Europæiske Fællesskabers finansielle interesser i henhold til konventionen af 26. juli 1995 om beskyttelse af De Europæiske Fællesskabers finansielle interesser
- ❑ organiseret eller væbnet tyveri
- ❑ ulovlig handel med kulturgoder, herunder antikviteter og kunstgenstande
- ❑ bedrageri
- ❑ afkrævning af beskyttelsespenge og pengeafpresning
- ❑ efterligninger og fremstilling af piratudgaver af produkter
- ❑ forfalskning af officielle dokumenter og ulovlig handel med falske dokumenter
- ❑ forfalskning af betalingsmidler
- ❑ ulovlig handel med hormonpræparater og andre vækstfremmende stoffer
- ❑ hvidvaskning af udbyttet fra strafbart forhold
- ❑ falskmøntneri, herunder forfalskning af euroen
- ❑ internetkriminalitet
- ❑ miljøkriminalitet, herunder
- ❑ ulovlig handel med truede dyrearter og ulovlig handel med truede plantearter og -sorter
- ❑ menneskesmugling
- ❑ forsætligt manddrab, grov legemsbeskadigelse
- ❑ ulovlig handel med menneskevæv og -organer
- ❑ bortførelse, frihedsberøvelse og gidseltagning
- ❑ racisme og fremmedhad
- ❑ ulovlig handel med nukleare og radioaktive materialer
- ❑ handel med stjålne motorkøretøjer
- ❑ voldtægt
- ❑ forsætlig brandstiftelse
- ❑ strafbare handlinger omfattet af Den Internationale Straffedomstols straffemyndighed
- ❑ skibs- eller flykapring
- ❑ sabotage

→ Lovovertrædelsen falder derfor ind under artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA → Artikel 4, stk. 1 (hastende sager), og artikel 4, stk. 3 (ikke-hastende sager), i rammeafgørelse 2006/960/RIA finder derfor anvendelse med hensyn til de tidsfrister, der skal overholdes i forbindelse med besvarelsen af denne anmodning

eller

❑ B — Lovovertrædelsen/lovovertrædelserne er ikke dækket af A.
I så fald gives en beskrivelse af lovovertrædelsen/lovovertrædelserne:

Formålet med anmodningen om oplysninger eller efterretninger

Forbindelsen mellem det formål, som oplysningerne eller efterretningerne skal bruges til, og den person, som er genstand for oplysningerne eller efterretningerne

Identiteten (hvis kendt) af den eller de personer, som står i centrum for den kriminalefterforskning eller kriminalefterretningsoperation, der ligger til grund for anmodningen om oplysninger eller efterretninger

Forhold, der giver anledning til at tro, at oplysningerne eller efterretningerne findes i den anmodede medlemsstat

Begrænsninger i brugen af oplysningerne i denne anmodning til andre formål end dem, hvortil de er meddelt, eller med henblik på forebyggelse af en umiddelbar og alvorlig trussel mod den offentlige sikkerhed

- ❑ kan bruges
- ❑ kan bruges, men den person, der har stillet oplysningerne til rådighed, må ikke nævnes
- ❑ kan ikke bruges uden tilladelse fra den person, der har stillet oplysningerne til rådighed
- ❑ kan ikke bruges

Figur 2

ANMODNING OM OPLYSNINGER OG EFTERRETNINGER

i henhold til Rådets rammeafgørelse 2006/960/RIA

I - Administrative oplysninger

Den anmodende medlemsstat:	
Den anmodende myndighed (navn, adresse, tlf., fax, e-mail):	
Oplysninger om sagsbehandler *(fakultativt)***:**	
Dato og klokkeslæt for anmodningen:	
Anmodningens referencenummer:	
Tidligere referencenumre:	

Den eller de anmodede medlemsstater:		
Kanal		
☐ENU/Europolforbindelsesofficer	☐Til orientering	☐Til imødekommelse
☐INTERPOL's NCB	☐Til orientering	☐Til imødekommelse
☐SIRENE	☐Til orientering	☐Til imødekommelse
☐Forbindelsesofficer	☐Til orientering	☐Til imødekommelse
☐Andet (angiv hvilket):	☐Til orientering	☐Til imødekommelse

II - Hastende karakter

Der anmodes om hastebehandling	☐ Ja ☐ Nej
Grunde til hastebehandling (f.eks. at mistænkte er varetægtsfængslet, eller at sagen skal for retten inden en bestemt dato):	
Overtrædelse omhandlet i artikel 2, stk. 2, i Rådets rammeafgørelse 2002/584/RIA om den europæiske arrestordre	☐ Ja ☐ Nej

III - Formål

Type af kriminalitet eller kriminel(le) aktivitet(er), der efterforskes
Beskrivelse af - de omstændigheder, som overtrædelsen eller overtrædelserne blev begået under (f.eks. tid, sted og i hvilken udstrækning den person, der er omfattet af anmodningen om oplysninger eller efterretninger, er meddelagtig i overtrædelsen eller overtrædelserne) - forhold, der giver anledning til at tro, at oplysningerne eller efterretningerne findes i den anmodede medlemsstat - forbindelsen mellem det formål, som oplysningerne eller efterretningerne skal bruges til, og den person, som er genstand for oplysningerne eller efterretningerne
☐ anmodning om at benytte oplysningerne som bevismateriale, hvis det er muligt i henhold til national ret *(fakultativt)*

IV - Oplysningernes art

Identiteten (hvis kendt) af den eller de pågældende personer eller genstande	
Personer	Genstand(e)
Efternavn: Fødenavn: Fornavn: Fødselsdato: Fødested: Køn: ☐ mand ☐ kvinde ☐ ubekendt Nationalitet: Yderligere oplysninger:	Våbnets serienummer: Dokumentnummer: Andet identifikationsnummer eller - navn: Køretøjets registreringsnummer: Køretøjets identifikationsnummer (VIN): Type dokumenter: Selskabets kontaktoplysninger (telefonnummer, e-mail, adresse www ...): Yderligere oplysninger:

De ønskede oplysninger eller efterretninger		
Personer	Køretøj	Andet
☐ verifikation af identitet ☐ screening i databaser ☐ konstatering af adresse/opholdssted	☐ supplering af identifikationsoplysninger ☐ identifikation af ejer ☐ identifikation af fører ☐ screening i databaser	☐ identifikation af selskab ☐ screening af selskabet i databaser ☐ screening af dokumenter i databaser ☐ identifikation af telefon-/faxnummer ☐ identifikation af indehaver af e-mailadressen ☐ screening af adresse ☐ screening af våben ☐ våbens handelsrute
Andet:		

V - Håndteringskoder

Begrænsninger i brugen af oplysningerne i denne anmodning til andre formål end dem, hvortil de er meddelt, eller med henblik på forebyggelse af en umiddelbar og alvorlig trussel mod den offentlige sikkerhed
☐ kun til brug for politiet, ikke til brug i retssager ☐ kontakt den, der har afgivet oplysningerne, inden enhver form for anvendelse

3.3. Schengen - Udveksling af SIS II-oplysninger og ikke-SIS II-oplysninger

Schengenaftalen, der blev undertegnet den 14. juni 1985, blev suppleret med konventionen om gennemførelse af Schengenaftalen (SGK)[74] i 1990, hvorved Schengenområdet blev oprettet gennem en afskaffelse af grænsekontrollen mellem Schengenlandene, fælles regler for visum samt politisamarbejde og retligt samarbejde. SGK fastsætter et generelt krav om politisamarbejde og bemyndiger politimyndighederne til at udveksle oplysninger inden for rammerne af landenes respektive retsordener.

Med Amsterdamtraktatens ikrafttræden i 1999 blev samarbejdsforanstaltninger, der indtil da var omfattet af Schengenreglerne, integreret i Den Europæiske Unions retlige ramme, og Schengenrelaterede spørgsmål behandles nu af EU's lovgivende organer. Schengenprotokollen, der er knyttet som bilag til Amsterdamtraktaten, fastsætter de nærmere ordninger for denne integrationsproces.

Schengeninformationssystemet (SIS) blev oprettet i henhold til bestemmelserne i afsnit IV i konventionen af 19. juni 1990. Det udgør et væsentligt redskab i forbindelse med anvendelsen af Schengenreglerne. Det udgør også en foranstaltning, der sigter mod at kompensere for, at der ikke foretages personkontrol inden for Schengenområdet, ved hjælp af et redskab til informationsudveksling mellem de kompetente myndigheder.

Det faktum, at den retlige ramme for SIS i øjeblikket består af to særskilte instrumenter, det vil sige en forordning for så vidt angår brugen af SIS ved grænserne og en rådsafgørelse for så vidt angår politisamarbejdet, berører ikke det forhold, at SIS udgør ét enkelt informationssystem.

---

[74] Konvention 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 (EFT L 239 af 22.9.2000, s. 19).

Lovgivning

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).

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).

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

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

Centrale bestemmelser

Schengeninformationssystemet (SIS) er et system for både politisamarbejde og grænsekontrol og støtter det operationelle samarbejde mellem politimyndigheder og judicielle myndigheder i straffesager. Udpegede politifolk, grænsevagter, toldere samt visummyndigheder og judicielle myndigheder i hele Schengenområdet kan konsultere SIS.[75]

Den anden generation af Schengeninformationssystemet ("SIS II") er for øjeblikket i drift i 26 EU-medlemsstater samt i de fire ikke-EU-lande, der er associeret til Schengensamarbejdet: Norge, Island, Schweiz og Liechtenstein.

[75] En konsolideret liste over nationale kompetente myndigheder med angivelse af, for hver myndighed, hvilke oplysninger den må søge og til hvilke formål, offentliggøres hvert år i Den Europæiske Unions Tidende i medfør af artikel 31, stk. 8, i SIS II-forordningen og artikel 46, stk. 8 i SIS II-afgørelsen.

- Hvad angår politisamarbejde, har både Det Forenede Kongerige og Irland anmodet om at få tilladelse til at deltage heri, men kun Det Forenede Kongerige fik i 2015 bemyndigelse til midlertidigt at indlæse data fra den pågældende del af SIS[76] som et første skridt, så der kan foretages en evaluering, inden der træffes en endelig "anvendelsesafgørelse". Det Forenede Kongerige og Irland deltager ikke i anvendelsen af SIS med henblik på grænsekontrol.

- Bulgarien, Rumænien[77] og Kroatien[78] anvender Schengenreglernes bestemmelser om politisamarbejde og grænsekontrol. De har fået direkte adgang til SIS med henblik på at evaluere, om Schengenreglernes bestemmelser om SIS anvendes korrekt. Når disse evalueringer er blevet foretaget på tilfredsstillende vis, vil en separat rådsafgørelse fastsætte datoen for ophævelse af kontrollen ved de indre grænser. Indtil da vil der fortsat være visse restriktioner for anvendelsen af SIS.

- Cypern har endnu ikke adgang til SIS.

Der kan søges i SIS II-oplysninger online (under overholdelse af strenge databeskyttelsesregler) døgnet rundt via SIRENE-kontorerne, ved grænsekontrolsteder, inden for nationalt territorium og på konsulater i udlandet. Oplysninger betegnes som indberetninger, der er et sæt oplysninger, som gør det muligt for myndighederne at identificere **personer**, dvs. EU-borgere og ikke-EU-borgere, eller **genstande** med henblik på at træffe passende forholdsregler til bekæmpelse af kriminalitet og irregulær indvandring.

Særligt bemyndiget Europolpersonale har inden for rammerne af sit mandat ret til direkte adgang til og søgning i oplysninger, der er indlæst i SIS II, og kan anmode om yderligere oplysninger fra den pågældende medlemsstat.

De nationale medlemmer af Eurojust og deres assistenter har inden for rammerne af deres mandat ret til adgang til og søgning i oplysninger, der er indlæst i SIS II.

---

[76] Rådets gennemførelsesafgørelse (EU) 2015/215 af 10. februar 2015 om iværksættelse af bestemmelserne i Schengenreglerne vedrørende databeskyttelse og om midlertidig iværksættelse af nogle af Schengenreglerne vedrørende Schengeninformationssystemet for Det Forenede Kongerige Storbritannien og Nordirland (EUT L 36 af 12.2.2015, s. 8).

[77] 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).

[78] 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).

I henhold til artikel 47 i SGK er forbindelsesofficerer, der er udstationeret ved andre Schengenlandes eller tredjelandes politi, ansvarlige for udvekslingen af oplysninger i medfør af:

- artikel 39, stk. 1, 2 og 3, under overholdelse af national ret med henblik på forebyggelse og opklaring af strafbare handlinger

- artikel 46, selv på eget initiativ, med henblik på forebyggelse af strafbare handlinger eller handlinger, der udgør en trussel mod den offentlige orden og sikkerhed.

Det skal bemærkes, at bestemmelserne i artikel 39, stk. 1, 2 og 3, og i artikel 46, i det omfang de vedrører udveksling af oplysninger og efterretninger i forbindelse med grov kriminalitet, erstattes af bestemmelserne i Rådets rammeafgørelse 2006/960/RIA, "den svenske rammeafgørelse". Dog finder bestemmelserne i artikel 39, stk. 1, 2 og 3, og i artikel 46 fortsat anvendelse for så vidt angår lovovertrædelser, der straffes med op til 12 måneders fængsel.

3.4. Europol

Lovgivning

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) (gældende fra 1. maj 2017).

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

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

Centrale bestemmelser

Formålet med Europol er at støtte og styrke indsatsen fra medlemsstaternes kompetente myndigheder med ansvar for forebyggelse og bekæmpelse af kriminalitet samt deres gensidige samarbejde om forebyggelse og bekæmpelse af organiseret kriminalitet, terrorisme og andre former for grov kriminalitet, der berører to eller flere medlemsstater. Med henblik herpå indsamler, lagrer, behandler, analyserer og udveksler Europol oplysninger og kriminalefterretninger.

Hver medlemsstat udpeger en national enhed (ENU), der fungerer som forbindelsesled mellem Europol og medlemsstaternes kompetente myndigheder. De nationale enheder varetager opgaver vedrørende udveksling af relevante oplysninger og efterretninger. Hver nationale enhed udstationerer mindst én forbindelsesofficer, der fungerer som det nationale forbindelseskontor ved Europol og varetager den nationale enheds interesser. Forbindelsesofficererne har til opgave at udveksle oplysninger mellem på den ene side medlemsstaterne og Europol og på den anden side bilateralt mellem andre lande. Disse bilaterale udvekslinger kan omfatte kriminalitet, der ligger uden for Europols mandat.

Europolforordningen introducerer et nyt databehandlingskoncept, som almindeligvis benævnes det integrerede datastyringskoncept (Integrated Data Management Concept (IDMC)). IDMC kan defineres som muligheden for at anvende oplysninger vedrørende kriminalitet til flere forskellige forretningsformål som anført af dataejeren, hvilket giver mulighed for at administrere og behandle dem på en integreret, teknologineutral måde. I Rådets Europolafgørelse var databehandlingen struktureret omkring systemer. Europolforordningen indeholder ikke længere henvisninger til systemer, men stiller i stedet krav om angivelse af formålet med behandlingen. For at lette overgangen kan brugere fortsat arbejde med de eksisterende systemer på en måde, der er i overensstemmelse med den nye retlige ramme.

Den nationale enhed er ansvarlig for kommunikationen med Europols informationssystem (EIS), som anvendes til at behandle oplysninger, der er nødvendige for udførelsen af Europols opgaver. Den nationale enhed, forbindelsesofficerer og behørigt bemyndiget Europolpersonale har ret til at registrere oplysninger i systemerne og søge oplysninger heri. Oplysninger, der indlæses i EIS, anses generelt for at være meddelt med henblik på krydstjek (forordningens artikel 18, stk. 2, litra a) og analyser af strategisk eller tematisk art (forordningens artikel 18, stk. 2, litra b).

3.5. INTERPOL

Lovgivning

Statutterne for INTERPOL[79].

Regler om behandling af oplysninger[80].

Regler om informationskontrol og adgang til INTERPOL's akter.

Centrale bestemmelser

INTERPOL's mission er at fremme internationalt politisamarbejde med henblik på forebyggelse og bekæmpelse af kriminalitet gennem øget samarbejde og innovation i politi- og sikkerhedsspørgsmål. Der træffes foranstaltninger inden for rammerne af eksisterende medlemsstatsret og i ånden af verdenserklæringen om menneskerettigheder. Hver af de 190 medlemsstater har et nationalt centralbureau (NCB), der bemandes af sit eget højtuddannede retshåndhævelsespersonale.

Statutterne for INTERPOL er en international aftale, der bekræfter medlemsskabet for regeringerne i alle de lande, der deltog i deres vedtagelse i 1956, og fastlægger ansøgningsproceduren for lande, der ikke blev medlem i 1956, med henblik på tiltrædelse af INTERPOL.

Som det primære retlige dokument fastsætter statutterne INTERPOL's mål og målsætninger. De fastlægger organisationens mandat til at sikre det bredest mulige samarbejde mellem alle kriminalpolitimyndigheder og bekæmpe almindelig kriminalitet.

Foruden statutterne udgør en række grundlæggende tekster INTERPOL's retlige ramme. Flere kontrolniveauer er blevet indført for at sikre overensstemmelse med reglerne. Disse vedrører kontroller foretaget af nationale centralbureauer (NCB), af generalsekretariatet og af den uafhængige instans for kontrol af INTERPOL's akter, Commission for the Control of INTERPOL's Files.

---

79 http://www.interpol.int/en/About-INTERPOL/Legal-materials/The-Constitution

80 http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts

3.6. Forbindelsesofficerer

Lovgivning

Konvention af 19. juni 1990 om gennemførelse af Schengenaftalen (SGK)[81], artikel 47.

Rådets afgørelse 2003/170/RIA af 27. februar 2003 om fælles benyttelse af forbindelsesofficerer udsendt af medlemsstaternes retshåndhævende myndigheder[82].

Rådets afgørelse 2006/560/RIA af 24. juli 2006 om ændring af afgørelse 2003/170/RIA om fælles benyttelse af forbindelsesofficerer udsendt af medlemsstaternes retshåndhævende myndigheder[83].

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) (gældende fra 1. maj 2017).

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

Bilaterale aftaler.

Centrale bestemmelser

Artikel 47 i SGK fastsætter, at medlemsstaterne "kan indgå bilaterale aftaler om tidsbegrænset eller tidsubegrænset udstationering af forbindelsesofficerer ved en anden [medlemsstats] politi." Forbindelsesofficererne er ikke bemyndiget til at udføre politiopgaver på egen hånd, og artikel 47 fastsætter, at sådanne udstationeringer "har til formål at fremme og fremskynde samarbejdet, navnlig ved

a) at bistå med informationsudvekslingen med henblik på såvel forebyggelse som bekæmpelse af kriminalitet

---

81 Konvention af 19. juni 1990 om gennemførelse af Schengenaftalen (SGK) (EFT L 239 af 22.9.2000, s. 19).
82 Rådets afgørelse 2003/170/RIA af 27. februar 2003 (EUT L 67 af 12.3.2003, s. 27).
83 Rådets afgørelse 2006/560/RIA af 24. juli 2006 (EUT L 219 af 10.8.2006, s. 31).

b) at bistå med efterkommelse af anmodninger om gensidig retshjælp mellem landenes politi og retsvæsen i straffesager

c) at yde bistand til de myndigheder, der har til opgave at overvåge de ydre grænser."

Der kan findes flere oplysninger om sådanne udstationeringer i "fodboldhåndbogen"[84] og i Rådets henstilling af 6. december 2007 om håndbogen for politi og sikkerhedsmyndigheder vedrørende samarbejde ved større arrangementer med en international dimension[85].

Bestemmelsen i SGK om, at nationale forbindelsesofficerer tillige kan varetage en eller flere andre medlemsstaters interesser, uddybes yderligere i Rådets afgørelse om fælles benyttelse af forbindelsesofficerer udsendt af medlemsstaternes retshåndhævende myndigheder (ændret i 2006). Der er også taget skridt til forbedring af samarbejdet mellem de forskellige medlemsstaters forbindelsesofficerer på deres udstationeringssted. Det er i forskellige fora blevet understreget, at dette samarbejde bør fremmes.

I overensstemmelse med Europolforordningen udpeger hver medlemsstat en national enhed (ENU), der fungerer som forbindelsesled mellem Europol og medlemsstaternes kompetente myndigheder, som har kompetence med hensyn til forebyggelse og bekæmpelse af strafbare handlinger. De nationale enheder varetager opgaver vedrørende udveksling af relevante oplysninger og efterretninger. Hver nationale enhed udstationerer mindst én forbindelsesofficer, der fungerer som det nationale forbindelseskontor ved Europol og varetager den nationale enheds interesser. Forbindelsesofficererne har til opgave at udveksle oplysninger mellem på den ene side den nationale enhed og Europol og på den anden side bilateralt mellem andre nationale enheder. Disse bilaterale udvekslinger kan omfatte kriminalitet, der ligger uden for Europols mandat.

Rådets afgørelse 2008/615/RIA ("Prümafgørelsen") fastsætter i artikel 17 og 18 bestemmelser om udstationering af nationale embedsmænd med henblik på at opretholde den offentlige orden og sikkerhed og forebygge strafbare handlinger.

---

84 Rådets resolution af 3. juni 2010 vedrørende en ajourført håndbog med henstillinger for det internationale politisamarbejde og foranstaltninger med henblik på forebyggelse og bekæmpelse af vold og uroligheder i forbindelse med fodboldkampe med international dimension, som mindst en medlemsstat deltager i (EUT C 165 af 24.6.2010, s. 1).

85 EUT C 314 af 22.12.2007, s. 4.

3.7. Udveksling af oplysninger i henhold til Prüm

Lovgivning

- Rådets afgørelse 2008/615/RIA af 23. juni 2008 om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet.

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

Centrale bestemmelser

Medlemsstaterne indrømmer gensidigt grænseoverskridende onlineadgang til referencedata for udpegede nationale DNA-analysedatabaser og elektroniske fingeraftryksidentifikationssystemer (AFIS) samt til oplysninger i køretøjsregistre (VRD) (jf. kapitel 2 i Rådets afgørelse 2008/615/RIA).

Der skal udpeges særlige nationale kontaktpunkter i hver medlemsstat. Der skal tages tilstrækkelig højde for bestemmelser om databeskyttelse og datasikkerhed i national ret. Den elektroniske sammenligning af anonyme biometriske profiler er baseret på et hit/no hit-system, undtagen i forbindelse med oplysninger i køretøjsregistre, hvor søgte oplysninger om ejer/bruger automatisk sendes tilbage.

I tilfælde af biometrisk overensstemmelse modtager den søgende medlemsstats nationale kontaktpunkt, i en elektronisk proces, de referencedata, som der er konstateret overensstemmelse med.

Der kan derefter anmodes om supplerende specifikke personoplysninger og yderligere oplysninger vedrørende referencedataene ved hjælp af procedurer for gensidig bistand, herunder de procedurer, der er vedtaget i medfør af "den svenske rammeafgørelse".

Den anmodede medlemsstats nationale ret, herunder bestemmelserne om retshjælp, finder anvendelse på leveringen af sådanne yderligere oplysninger. Det er underforstået, at levering af personoplysninger kræver et passende databeskyttelsesniveau fra den modtagende medlemsstats side[86].

Med henblik på forebyggelse af strafbare handlinger og opretholdelse af den offentlige orden og sikkerhed i forbindelse med store arrangementer med en grænseoverskridende dimension kan medlemsstaterne både efter anmodning og på eget initiativ levere både andre oplysninger end personoplysninger og personoplysninger til hinanden. Til dette formål udpeges der særlige nationale kontaktpunkter (NCP) (jf. kapitel 3 i Rådets afgørelse 2008/615/RIA).

Med henblik på forebyggelse af terrorforbrydelser kan medlemsstaterne under visse omstændigheder levere personoplysninger til hinanden. Til dette formål udpeges der særlige nationale kontaktpunkter (jf. kapitel 4 i Rådets afgørelse 2008/615/RIA).

3.8. Visuminformationssystemet (VIS)

Lovgivning

Rådets beslutning 2004/512/EF af 8. juni 2004 om indførelse af visuminformationssystemet (VIS) (EUT L 213 af 15.6.2004, s. 5).

Rådets afgørelse 2013/392/EU om fastsættelse af den dato, fra hvilken afgørelse 2008/633/RIA om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger har virkning (EUT L 198 af 23.7.2013, s. 45)[87].

---

[86] Rådets afgørelse 2008/615/RIA overholder det beskyttelsesniveau, der er fastsat for behandling af personoplysninger i Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, tillægsprotokollen af 8. november 2001 til konventionen og principperne i Europarådets anbefaling R (87) 15 om politiets brug af personoplysninger.

[87] EU-Domstolen annullerede den 16. april 2015 Rådets afgørelse 2013/392/EU af 22. juli 2013 om fastsættelse af den dato, fra hvilken afgørelse 2008/633/RIA om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger har virkning. Domstolen erklærede dog, at virkningerne af afgørelse 2013/392/EU opretholdes indtil ikrafttrædelsen af en ny retsakt, der erstatter den.

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

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

Centrale bestemmelser

VIS er et system, som giver de kompetente nationale myndigheder mulighed for at indlæse og opdatere (såkaldte Schengen-)visumdata til kortvarigt ophold og konsultere dem elektronisk. Det er baseret på en centraliseret arkitektur og består af et centralt informationssystem, det centrale visuminformationssystem (CS-VIS), en national grænseflade i hver medlemsstat (NI-VIS) og kommunikationsinfrastrukturen mellem det centrale visuminformationssystem og de nationale grænseflader. Afgørelse 2008/633/RIA gør det muligt at anvende VIS til at forebygge, afsløre og efterforske terrorhandlinger og andre alvorlige strafbare handlinger. Det gør det muligt for de udpegede retshåndhævende myndigheder (f.eks. myndigheder med ansvar for bekæmpelse af terrorisme eller alvorlige strafbare handlinger, f.eks. narkotikahandel eller menneskehandel) i landene i Schengenområdet og Europol at få adgang til VIS. De udpegede nationale myndigheder skal følge en procedure for at få adgang til VIS, når alle adgangsbetingelser er opfyldt.

I maj 2018 forelagde Kommissionen et lovgivningsforslag om ændring af VIS-forordningen, der bl.a. tager sigte på at sikre interoperabilitet mellem andre databaser inden for RIA-området, som registrerer visum til længerevarende ophold og opholdstilladelser i VIS. Forslaget indeholder også og videreudvikler bestemmelserne for retshåndhævende myndigheders adgang til VIS og ophæver afgørelse 2008/633/RIA.

Det opgraderede VIS forventes ikke at være operationelt inden udgangen af 2021.

3.9. Eurodac

Lovgivning

Det europæiske automatiske fingeraftryksidentifikationssystem (Eurodac) er et computersystem, der oprindeligt havde til formål at fremme den effektive anvendelse af Dublinkonventionen. Dublinkonventionen, der blev undertegnet den 15. juni 1990, blev erstattet af Rådets forordning (EF) nr. 343/2003 af 18. februar 2003 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en asylansøgning, der er indgivet af en tredjelandsstatsborger i en af medlemsstaterne.

Efter de ændringer, der er foretaget i forordningerne om Eurodac, blev de omarbejdet ved

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

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

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

Centrale bestemmelser

Forordning (EU) nr. 603/2013 fastsætter formålet med Eurodac og definerer betingelserne for de udpegede nationale retshåndhævende myndigheders og Europols adgang til Eurodacoplysninger med henblik på at forebygge, opdage eller efterforske terrorhandlinger[88] eller andre alvorlige lovovertrædelser[89].

3.10. Napoli II

Lovgivning

Rådets retsakt af 18. december 1997 om udarbejdelse, på grundlag af artikel K.3 i traktaten om Den Europæiske Union, af konventionen om gensidig bistand og samarbejde mellem toldmyndighederne (EFT C 24 af 23.1.1998, s. 1).

Centrale bestemmelser

Medlemsstaterne yder hinanden gensidig bistand med henblik på at forebygge og efterforske overtrædelser af nationale toldbestemmelser og forfølge og straffe overtrædelser af EF- toldbestemmelser og nationale toldbestemmelser. Inden for rammerne af kriminalefterforskninger fastlægger Napoli II-konventionen procedurer, som gør det muligt for toldmyndighederne at handle i fællesskab og udveksle oplysninger, uden forudgående anmodning eller efter anmodning, om ulovlig handel.

Anmodningerne fremsættes skriftligt på et officielt sprog i den bistandssøgte myndigheds medlemsstat eller på et for denne myndighed acceptabelt sprog. Standard for meddelelsen af oplysninger fastsættes i en formular. De berørte myndigheder meddeler alle oplysninger, der kan være nyttige i forbindelse med at forebygge, afsløre og forfølge overtrædelser. De udveksler personoplysninger, dvs. alle oplysninger om en identificeret eller identificerbar fysisk person.

Ved ydelse af bistand optræder den bistandssøgte myndighed eller den kompetente myndighed, som førstnævnte har indbragt sagen for, på samme måde, som hvis den handlede på egne vegne eller efter anmodning fra en anden myndighed i sit hjemland.

---

88 Rådets rammeafgørelse 2002/475/RIA af 13. juni 2002 om bekæmpelse af terrorisme (EFT L 164 af 22.6.2002, s. 3).

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

3.10.1. Toldinformationssystemet - CIS[90]

Toldinformationssystemet supplerer Napoli II-konventionen[91]. Det centraliserede informationssystem forvaltes af Kommissionen og sigter mod at styrke medlemsstaternes toldmyndigheder gennem hurtig udveksling af oplysninger med henblik på at forebygge, efterforske og retsforfølge alvorlige overtrædelser af national ret og EU-retten. Med CIS oprettes også et elektronisk sagsregister på toldområdet (FIDE) til bistand for toldefterforskninger.

De myndigheder, der er udpeget af medlemsstaterne[92], har direkte adgang til oplysningerne i CIS. For at øge komplementariteten med Europol og Eurojust har begge organer læseadgang til CIS og FIDE.

CIS omfatter personoplysninger i forbindelse med råvarer, transportmidler, virksomheder, personer og varer og likvide midler, der er tilbageholdt, beslaglagt eller konfiskeret. Personoplysninger må kun kopieres fra CIS til andre databehandlingssystemer til risikostyring eller operationelle analyser, som kun analytikere udpeget af medlemsstaterne har adgang til.

FIDE giver de nationale myndigheder, der har ansvaret for at foretage toldefterforskning, mulighed for, når de åbner en efterforskningssag, at identificere andre myndigheder, der måtte have efterforsket en bestemt person eller virksomhed.

3.11. Nationale kontorer for inddrivelse af aktiver (ARO) og CARIN

Lovgivning

Rådets afgørelse 2007/845/RIA af 6. december 2007 om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet (EUT L 332 af 18.12.2007, s. 103).

Camden Assets Recovery Inter-Agency Network (CARIN) (Camdennettet for kompetente myndigheder med hensyn til inddrivelse af aktiver) blev oprettet i Haag den 22.-23. september 2004 af Østrig, Belgien, Tyskland, Irland, Nederlandene og Det Forenede Kongerige.

---

90 Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet (EUT L 323 af 10.12.2009, s. 20).

91 Konvention, udarbejdet på grundlag af artikel K.3 i traktaten om Den Europæiske Union, om gensidig bistand og samarbejde mellem toldmyndighederne (EFT C 24 af 23.1.1998, s. 2).

92 Gennemførelse af artikel 7, stk. 2, og artikel 8, stk. 3, i Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet – ajourførte lister over kompetente myndigheder (13394/11 ENFOCUSTOM 85).

Centrale bestemmelser

Efter vedtagelsen af Rådets afgørelse 2007/845/RIA[93] har alle medlemsstater oprettet og udpeget kontorer for inddrivelse af aktiver (ARO'er). De kan udveksle oplysninger om spørgsmål vedrørende inddrivelse af aktiver direkte via SIENA-systemet. Under ledelse af Europa-Kommissionen og Europol fremmer ARO-netværket samarbejdet mellem medlemsstaternes kontorer for inddrivelse af aktiver samt strategiske drøftelser og udveksling af bedste praksis. Europols kontor for formuegoder forbundet med kriminalitet (ECAB) fungerer som fokuspunkt for inddrivelse af aktiver i EU.

Bestemmelserne i Europa-Parlamentets og Rådets direktiv 2014/42/EU af 3. april 2014 om indefrysning og konfiskation af redskaber og udbytte fra strafbart forhold i Den Europæiske Union[94] vil yderligere forbedre effektiviteten af samarbejdet mellem kontorerne for inddrivelse af aktiver i Den Europæiske Union. Medlemsstaterne opfordres til at gennemføre direktivet i national ret senest den 4. oktober 2016.

Camden Assets Recovery Inter-Agency Network (CARIN), der blev oprettet i 2004 for at støtte grænseoverskridende identifikation, indefrysning, beslaglæggelse og konfiskation af formuegoder forbundet med kriminalitet, styrker den gensidige udveksling af oplysninger om forskellige nationale tilgange, der går ud over EU.

CARIN-nettet omfatter pr. 2015 aktører fra 53 jurisdiktionsområder og ni internationale organisationer, der fungerer som kontaktpunkter med henblik på hurtig grænseoverskridende udveksling af oplysninger efter anmodning eller uanmodet. De nationale kontorer for inddrivelse af aktiver samarbejder indbyrdes eller med andre myndigheder, der letter opsporing og identificering af udbytte fra strafbart forhold. Alle medlemsstater har oprettet et kontor for inddrivelse af aktiver, men der er store forskelle mellem medlemsstaterne med hensyn til organisatorisk opbygning, ressourcer og aktiviteter.

---

93 Rådets afgørelse 2007/845/RIA af 6. december 2007 om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet (EUT L 332 af 18.12.2007, s. 103).

94 Europa-Parlamentets og Rådets direktiv 2014/42/EU af 3. april 2014 om indefrysning og konfiskation af redskaber og udbytte fra strafbart forhold i Den Europæiske Union (EUT L 127 af 29.4.2014, s. 39).

De oplysninger, der udveksles, kan benyttes i henhold til bestemmelserne om databeskyttelse i de modtagende medlemsstater og er omfattet af de samme regler for databeskyttelse, som hvis oplysningerne var indsamlet i den modtagende medlemsstat. Uanmodet udveksling af oplysninger i henhold til denne afgørelse og under anvendelse af de procedurer og tidsfrister, der er fastsat i den svenske rammeafgørelse, skal fremmes.

3.12. Finansielle efterretningsenheder (FIU)

Lovgivning

Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF
(EUT L 141 af 5.6.2015, s. 73)

Europa-Parlamentets og Rådets direktiv (EU) 2019/1153 af 20. juni 2019 om regler, der letter brugen af finansielle og andre oplysninger med henblik på forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger, og om ophævelse af Rådets afgørelse 2000/642/RIA
(EUT L 186 af 11.7.2019, s. 122)

Centrale bestemmelser

I henhold til direktiv 2015/849 (4. hvidvaskdirektiv som ændret ved direktiv 2018/843) opretter hver medlemsstat en FIU for at forebygge, opdage og effektivt bekæmpe hvidvask af penge og finansiering af terrorisme. FIU'en er som central national enhed ansvarlig for at modtage og analysere indberetninger af mistænkelige transaktioner og andre oplysninger af relevans for hvidvask af penge, tilknyttede underliggende forbrydelser eller finansiering af terrorisme. FIU'en er ansvarlig for at formidle resultaterne af sin analyse og alle yderligere relevante oplysninger til de kompetente myndigheder, når der er begrundet mistanke om hvidvask af penge, tilknyttede underliggende forbrydelser eller finansiering af terrorisme. Den skal kunne indhente yderligere oplysninger hos forpligtede enheder. FIU'er skal kunne imødekomme anmodninger om oplysninger fra kompetente myndigheder i deres respektive medlemsstat, når disse anmodninger om oplysninger er affødt af bekymringer vedrørende hvidvask af penge, tilknyttede underliggende forbrydelser eller finansiering af terrorisme.

Ud over ovennævnte udveksling af oplysninger om hvidvask af penge og finansiering af terrorisme fastsætter direktiv (EU) 2019/1153, at hver medlemsstat skal sikre, at dens nationale FIU også forpligtes til at samarbejde med den pågældende stats udpegede retshåndhævende myndigheder og være i stand til at svare på deres begrundede anmodninger om finansielle oplysninger eller finansielle analyser, når sådanne anmodninger er begrundet i hensynet til forebyggelse, afsløring, efterforskning eller retsforfølgning af alvorlige strafbare handlinger, som defineret i bilag 1 til Europolforordningen (2016/794).

I begge tilfælde kan FIU nægte at udlevere oplysningerne, når der er objektive grunde til at formode, at det vil få en negativ indvirkning på igangværende efterforskninger, eller hvis videregivelse af oplysningerne vil stå i klart misforhold til en fysisk eller juridisk persons legitime interesser eller være irrelevant i forhold til formålet med anmodningen.

I henhold til direktiv 2015/849 (hvidvaskdirektivet) sikrer medlemsstaterne, at FIU'er uopfordret eller efter anmodning indbyrdes udveksler alle oplysninger, som måtte være relevante for FIU'ernes behandling eller analyse af oplysninger om hvidvask af penge eller finansiering af terrorisme og de fysiske eller juridiske personer, der er involveret, uanset typen af tilknyttet underliggende forbrydelse, også selv om det på tidspunktet for udvekslingen ikke er identificeret, hvilken tilknyttet underliggende forbrydelse der er tale om. En FIU kan kun i særlige tilfælde, hvor udvekslingen kan være i modstrid med grundlæggende principper i national ret i dens medlemsstat, nægte at udveksle oplysninger. Medlemsstaterne sikrer, at de oplysninger, der udveksles i henhold til artikel 52 og 53, kun anvendes til det formål, hvortil oplysningerne ønskedes eller blev udleveret.

Ud over udvekslingen mellem FIU'er i forskellige medlemsstater i henhold til direktiv 2015/849 fastsætter direktiv 2019/1153 nu, at FIU'erne i ekstraordinære og hastende tilfælde også er berettigede til at udveksle finansielle oplysninger eller finansielle analyser, der kan være relevante for behandling eller analyse af oplysninger vedrørende terrorisme eller organiseret kriminalitet, der er knyttet til terrorisme. Direktiv 2019/1153 tillader også udveksling af oplysninger mellem FIU'er og Europol.

FIU.NET er et decentralt computernetværk til udveksling af oplysninger mellem finansielle efterretningsenheder.

FIU.NET, der oprindeligt havde til formål at styrke de finansielle efterretningsenheders stilling, har over de seneste år udviklet sig fra et sikkert grundlæggende redskab til struktureret bilateral udveksling af oplysninger til et sikkert multifunktionelt redskab til multilateral udveksling af oplysninger med sagsbehandlingsfunktioner og halvautomatiseret standardisering af processer. I FIU.NET er hver ny funktion og automatiseret proces valgfri og uden forbehold. De enkelte FIU'er kan beslutte, hvilke af FIU.NET's muligheder og funktioner de vil bruge. De anvender kun de funktioner, som de føler sig trygge ved, og undlader at bruge dem, som de ikke har brug for eller ikke vil bruge.

3.13. Aftale mellem EU og USA om programmet til sporing af finansiering af terrorisme (TFTP)

Lovgivning

Aftale mellem Den Europæiske Union og Amerikas Forenede Stater om behandling og overførsel af finansielle betalingsdata fra Den Europæiske Union til USA til brug for programmet til sporing af finansiering af terrorisme

(EUT L 195 af 27.7.2010, s. 5)

Centrale bestemmelser

I kølvandet på 11. september besluttede EU og USA at arbejde tæt sammen og indgik aftalen om behandling og overførsel af finansielle betalingsdata fra Den Europæiske Union til USA til brug for programmet til sporing af finansiering af terrorisme (TFTP-aftalen mellem EU og USA). I henhold til aftalen udleverer det amerikanske finansministerium også TFTP-oplysninger til retshåndhævende myndigheder eller offentlige sikkerheds- eller antiterrormyndigheder i de berørte medlemsstater og, hvis det er relevant, til Europol og Eurojust.

TFTP indeholder strenge kontrolforanstaltninger for at sikre, at sikkerhedsforanstaltninger, herunder vedrørende privatlivets fred og beskyttelse af personoplysninger, overholdes. Oplysningerne behandles udelukkende med henblik på forebyggelse, efterforskning, opsporing eller retsforfølgning af terrorisme eller finansiering heraf. Med henblik på denne aftale kan det amerikanske finansministerium anmode om finansielle betalingsdata og dertil knyttede oplysninger, der opbevares på EU's område, fra udpegede udbydere af internationale finansielle betalingstjenester.

Fordelen ved TFTP-oplysninger for medlemsstaterne, Europol og Eurojust begrænses af det forhold, at analyse af grænseoverskridende betalinger under TFTP udelukkende er baseret på FIN-meddelelser (Financial Institution Transfer), som er en type SWIFT-meddelelser, hvorved finansielle oplysninger overføres fra en finansiel institution til en anden. Andre betalingsmetoder tages ikke i betragtning. TFTP er imidlertid den eneste mekanisme, der inden for et meget kort tidsrum gør det muligt at kortlægge og profilere transaktioner, som mistænkes for at være forbundet med terrorisme eller finansiering heraf, med henblik på at øge den interne sikkerhed. Som følge af en øget bevidsthed omkring gensidighedsklausulerne i denne aftale anvender EU's myndigheder i stigende grad denne mekanisme for således at nyde gavn af udvekslingen af oplysninger med USA. Det bør i denne forbindelse bemærkes, at alle anmodninger fra EU's myndigheder om TFTP-søgninger skal opfylde kravene i aftalens artikel 10.

Selv om aftalen ikke åbner mulighed for, at medlemsstaterne gennem Europol kan anmode om en søgning efter relevante oplysninger opnået via TFTP, vil det være nyttigt – med henblik på at forbedre EU's respons på terrorisme og finansiering heraf – hvis medlemsstaterne som minimum underretter Europol systematisk og rettidigt om deres direkte anmodninger i henhold til artikel 10. For at støtte medlemsstaterne i kanaliseringen af anmodninger om TFTP-søgninger har Europol oprettet et enkelt kontaktpunkt (SPOC), og med sine analyseregistre (AWF) og sit veletablerede samarbejde med finansministeriet er det godt rustet til at behandle medlemsstaternes anmodninger effektivt.

3.14. Udveksling af oplysninger fra strafferegistre (ECRIS)

Lovgivning

Rådets rammeafgørelse 2009/315/RIA af 26. februar 2009 om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne (EUT L 93 af 7.4.2009, s. 23). Denne rammeafgørelse ophæver Rådets afgørelse 2005/876/RIA af 21. november 2005 om udveksling af oplysninger fra strafferegistre (EUT L 322 af 9.12.2005, s. 33).

Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 171 af 7.6.2019, s. 143).

Centrale bestemmelser

Rådets rammeafgørelse 2009/315/RIA kræver, at en domsstat snarest muligt skal informere den eller de medlemsstater, hvori den pågældende person er statsborger, om domme, der er anført i dens strafferegister, samt om ændringer eller sletning af denne dom. Den medlemsstat, hvori den berørte person er statsborger, er forpligtet til at opbevare oplysningerne med henblik på videreformidling. Alle ændringer eller sletninger i domsstaten medfører en identisk ændring eller sletning i strafferegistret i den medlemsstat, hvor den pågældende person er statsborger Der kan anmodes om oplysninger om straffedomme fra den medlemsstat, hvori den pågældende person er statsborger, med henblik på straffesager eller andre formål end straffesager, såsom forebyggelse af en umiddelbar og alvorlig trussel mod den offentlige sikkerhed. Brugen af oplysninger, der videregives i henhold til denne afgørelse, til andre formål end en straffesag, kan imidlertid begrænses i overensstemmelse med den anmodede medlemsstats nationale ret og den anmodende medlemsstat for ikke at kompromittere social rehabilitering af den domfældte.

Rådets afgørelse 2009/316/RIA fastsætter de måder, hvorpå en medlemsstat skal overføre sådanne oplysninger. Rådets afgørelse fastsætter rammerne for et elektronisk system til udveksling af oplysninger fra strafferegistre. De centrale myndigheder i hver medlemsstat anvender de særlige anmodnings- og svarformularer, der er knyttet som bilag til rammeafgørelsen, i elektronisk form som beskrevet i lovgivningen.

3.14.1. Udveksling af oplysninger om tredjelandsstatsborgeres og statsløse personers straffeattester (ECRIS-TCN)

Lovgivning

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

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

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

Europa-Parlamentets og Rådets direktiv (EU) 2019/884 af 17. april 2019 om ændring af Rådets rammeafgørelse 2009/315/RIA for så vidt angår udveksling af oplysninger om tredjelandsstatsborgere og det europæiske informationssystem vedrørende strafferegistre (ECRIS) og om erstatning af Rådets afgørelse 2009/316/RIA (EUT L 171 af 7.6.2019, s. 143).

Centrale bestemmelser

Forordningen finder anvendelse på behandling af identitetsoplysninger om tredjelandsstatsborgere, der har været genstand for straffedomme i medlemsstaterne. Ved "tredjelandsstatsborger" forstås en person, der ikke er unionsborger som defineret i artikel 20, stk. 1, i TEUF, eller der er en statsløs person eller en person, hvis nationalitet er ukendt. Strafferegisteroplysninger om disse personer opbevares i domsstaten. Formålet med ECRIS-TCN[95] er at finde ud af, hvilke andre medlemsstater der ligger inde med sådanne strafferegisteroplysninger. ECRIS-rammen kan derefter anvendes til at anmode disse medlemsstater om sådanne oplysninger i overensstemmelse med rammeafgørelse 2009/315/RIA.

I forordningen fastsættes regler om oprettelse af et centralt system på EU-plan, der indeholder personoplysninger, som udvikles og vedligeholdes af eu-LISA, og regler om ansvarsfordelingen mellem medlemsstaten og den organisation, der er ansvarlig for udvikling og vedligeholdelse af det centraliserede system. Det fastsætter et passende samlet niveau for databeskyttelse, datasikkerhed og beskyttelse af de berørte personers grundlæggende rettigheder.

---

95 Kommissionen bestemmer, fra hvilken dato ECRIS-TCN skal idriftsættes, når betingelserne i artikel 35 i forordning (EU) 2019/816 er opfyldt.

Eurojust, Europol, og EPPO bør have adgang til ECRIS-TCN med henblik på at kunne bestemme, hvilke medlemsstater der ligger inde med strafferegisteroplysninger om en tredjelandsstatsborger, for at støtte dem i udførelsen af deres lovbestemte opgaver.

3.15. Lagring af telekommunikationsdata

Lovgivning

Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF[96].

Centrale bestemmelser

Direktivet finder anvendelse på udbydere af elektroniske kommunikationstjenester. Direktivet fastsætter, at udbydere skal lagre trafikdata og lokaliseringsdata samt lignende data, der er nødvendige for at identificere abonnenten eller brugeren, med henblik på at fremsende disse data til de kompetente nationale myndigheder efter anmodning. Med henblik på efterforskning, afsløring og retsforfølgning af alvorlige forbrydelser pålægger medlemsstaterne udbydere af elektroniske kommunikationstjenester eller af offentlige kommunikationsnet at lagre de kategorier af data, der er nødvendige for at identificere:

- kilden til en kommunikation
- kommunikationens bestemmelsessted
- kommunikationens dato, klokkeslæt og varighed
- kommunikationens type
- brugernes kommunikationsudstyr eller det, der fremstår som værende deres udstyr
- lokaliseringen af mobilt kommunikationsudstyr.

Data, der afslører indholdet af kommunikationen, må ikke lagres.

---

[96] Den Europæiske Unions Domstols dom af 8. april 2014 erklærede direktivet for ugyldigt.

3.16. Direktivet om passagerlister (PNR)

Lovgivning

Europa-Parlamentets og Rådets direktiv (EU) 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet

Centrale bestemmelser

Direktivet fastsætter på EU-plan en fælles retlig ramme for overførsel og behandling af PNR-oplysninger og indeholder bestemmelser om:

b) luftfartsselskabers[97] videregivelse af passagerlisteoplysninger (PNR-oplysninger) om passagerer på flyvninger uden for EU. Hvis en medlemsstat beslutter at anvende direktivet på interne flyvninger i EU, finder alle bestemmelser anvendelse på flyvninger inden for EU, som var de flyvninger uden for EU

c) behandlingen af PNR-oplysninger, herunder medlemsstaternes indsamling, anvendelse og tilbageholdelse, og udveksling mellem medlemsstaterne.

Med henblik på behandling af PNR-oplysninger opretter eller udpeger hver medlemsstat en kompetent myndighed, der skal fungere som dens passageroplysningsenhed (PIU). To eller flere medlemsstater kan oprette eller udpege en enkelt myndighed til at fungere som deres fælles PIU.

PNR-oplysninger, der er omhandlet i bilag I til direktivet, overføres til PIU'er, for så vidt de allerede er indsamlet af luftfartsselskaberne som led i deres normale aktiviteter. Nogle luftfartsselskaber opbevarer forhåndsinformation om passagerer (API) som en del af PNR-oplysningerne, mens andre ikke gør. Uanset hvordan luftfartsselskaberne indsamler API, skal de overføre API-oplysningerne til PIU'erne, der skal behandle dem på samme måde som PNR-oplysninger. Direktivets bilag II indeholder en liste over grove "overtrædelser", som er omfattet af direktivets anvendelsesområde.

---

[97] Direktivet påvirker ikke medlemsstaternes mulighed for at indføre et system i national ret til indsamling og behandling af PNR-oplysninger fra erhvervsdrivende, der ikke er luftfartsselskaber, f.eks. rejsebureauer og rejsearrangører, der leverer rejserelaterede tjenester, herunder reservation af flyvninger, for hvilke de indsamler og behandler PNR-oplysninger, eller fra andre transportvirksomheder end dem, der er nævnt i direktivet, forudsat at sådan national ret er i overensstemmelse med EU-retten.

Behandlingen af PNR-oplysninger tjener til at vurdere passagerer forud for deres ankomst til eller afrejse fra en medlemsstat for at identificere personer, som skal undersøges nærmere af de myndigheder, der har kompetence til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, og, hvor det er relevant, af Europol inden for rammerne af dets kompetence og med henblik på udførelsen af dets opgaver.

For at gennemføre vurderingen kan PIU'erne:

a) sammenholde PNR-oplysninger med oplysninger i databaser, der er relevante med henblik på at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, herunder databaser vedrørende personer eller genstande, der eftersøges eller er indberettet, i overensstemmelse med de EU-regler og internationale eller nationale regler, som finder anvendelse på sådanne databaser, eller

b) behandle PNR-oplysninger efter forud fastsatte kriterier.

På nationalt plan videregiver PIU'erne PNR-oplysninger eller resultaterne af behandlingen heraf til de kompetente nationale retshåndhævende myndigheder, der har ret til at foretage en nærmere undersøgelse af sagen eller træffe passende foranstaltninger for at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet. PIU'erne udgør den vigtigste grænseoverskridende informationsudvekslingskanal, men de kompetente myndigheder kan henvende sig direkte til PIU'er i en anden medlemsstat i nødsituationer og på nøje fastlagte betingelser.

På EU-plan udveksler PIU'er både PNR-oplysninger, der er indsamlet fra luftfartsselskaber, og resultatet af behandlingen af disse oplysninger indbyrdes og med Europol, der inden for rammerne af sine kompetencer og med henblik på at løse sine opgaver har ret til at anmode om sådanne oplysninger fra PIU'erne.

PNR-oplysninger skal opbevares i en database hos PIU'en i fem år efter overførslen fra den medlemsstat, hvor flyet ankom eller afgik. Alle PNR-oplysninger skal imidlertid anonymiseres efter en periode på seks måneder. Dette gøres ved hjælp af maskering af alle dataelementer, der kan tjene til direkte at identificere den passager, som dataene vedrører. Listen over PNR-oplysninger, der skal maskeres, findes i direktivet. Efter fem år skal PNR-oplysningerne slettes, medmindre de er blevet videregivet til en kompetent myndighed med henblik på at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, og de er i så fald underlagt national ret.

I overensstemmelse med EU-lovgivningen om databeskyttelse forbyder PNR-direktivet behandling af følsomme oplysninger om f.eks. race eller etnisk oprindelse, politiske anskuelser, religiøs eller filosofisk overbevisning, medlemskab af en fagforening, sundhed, seksualitet eller seksuel orientering.

3.17. Forhåndsinformation om passagerer (API)

Lovgivning

Rådets direktiv 2004/82/EF af 29. april 2004 om transportvirksomheders forpligtelse til at fremsende oplysninger om passagerer

Centrale bestemmelser

Direktivet tager sigte på at forbedre grænsekontrollen og bekæmpe ulovlig indvandring. Med henblik herpå kræver direktivet, at medlemsstaterne indfører en forpligtelse for luftfartsselskaberne til at meddele visse oplysninger om deres rejsende forud for deres indrejse i EU. Sådanne oplysninger benævnes forhåndsinformation om passagerer (API). På særlige betingelser og under særlige forhold kan medlemsstaterne også anvende API-oplysninger med henblik på retshåndhævelse.

Disse oplysninger gives på anmodning af de myndigheder, der er ansvarlige for personkontrollen ved EU's ydre grænser.

Luftfartsselskaberne bør fremsende API-oplysninger elektronisk eller, hvis dette ikke er muligt, på anden passende måde til de myndigheder, der foretager grænsekontrol, hvor passageren rejser ind i EU. API-oplysninger kontrolleres i nationale og europæiske databaser såsom Schengeninformationssystemet (SIS) og visuminformationssystemet (VIS).

Når API-oplysninger matcher en registrering i en database, sendes der en indberetning til grænsepolitiet, og der foretages en målrettet undersøgelse af den pågældende passager ved ankomsten.

Indsamlede og fremsendte API-oplysninger skal slettes af luftfartsselskaber og myndigheder inden for 24 timer efter fremsendelse eller ankomst. Grænsemyndighederne kan dog opbevare de midlertidige filer i mere end 24 timer, hvis oplysningerne senere er nødvendige for udøvelsen af de lovpligtige funktioner, som påhviler grænsemyndighederne, eller for at håndhæve love og administrative bestemmelser vedrørende indrejse og indvandring, herunder bestemmelserne heri om beskyttelse af den offentlige orden (ordre public) og den nationale sikkerhed.

3.18. Trafiksikkerhedsrelaterede færdselslovsovertrædelser

Lovgivning

Europa-Parlamentets og Rådets direktiv (EU) 2015/413 af 11. marts 2015 om fremme af grænseoverskridende udveksling af oplysninger om trafiksikkerhedsrelaterede færdselslovsovertrædelser (EUT L 68 af 13.3.2015, s. 9)

Centrale bestemmelser

Medlemsstaterne giver hinanden onlineadgang til oplysninger i deres nationale køretøjsregistre (VRD) med henblik på at håndhæve sanktioner for visse trafiksikkerhedsrelaterede lovovertrædelser begået med et køretøj, der er registreret i en anden medlemsstat end den medlemsstat, hvor overtrædelsen blev begået. Overtrædelsesmedlemsstaten anvender de oplysninger, der er indhentet, med henblik på at fastslå, hvem der er personligt ansvarlig for færdselslovsovertrædelsen. Udvekslingen af oplysninger finder anvendelse på:

- hastighedsovertrædelser
- undladelse af at bruge sikkerhedssele
- undladelse af at stoppe for rødt lyssignal
- spirituskørsel
- kørsel under påvirkning af stoffer
- undladelse af at bruge styrthjelm
- ulovlig brug af kørebane
- ulovlig brug af mobiltelefon eller anden kommunikationsanordning under kørslen.

Ved hjælp af den særlige softwareapplikation Eucaris giver medlemsstaterne deres udpegede nationale kontaktpunkter (NCP) gensidig adgang til oplysninger i køretøjsregistre med ret til at foretage automatiseret søgning af:

d) oplysninger vedrørende køretøjer og

e) oplysninger vedrørende køretøjers ejere eller indehavere.

3.19. Ind- og udrejsesystemet (EES)

Lovgivning

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

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

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

Forordningen udgør en udvikling af bestemmelser i Schengenreglerne.

Danmark meddelte, at det i medfør af artikel 4 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, har truffet afgørelse om at gennemføre ovennævnte forordninger i dansk ret. Denne afgørelse skaber en forpligtelse i henhold til folkeretten mellem Danmark og de øvrige medlemsstater, der er bundet af foranstaltningerne.

Det Forenede Kongerige og Irland deltager ikke i gældende EU-ret, og forordningen er derfor ikke bindende for og finder ikke anvendelse i Det Forenede Kongerige og Irland.

Gældende EU-ret er bindende for Island, Norge, Liechtenstein og Schweiz i henhold til de respektive aftaler eller protokollen vedrørende Schengenreglerne.

For så vidt angår Cypern, Bulgarien, Rumænien og Kroatien udgør forordningens bestemmelser vedrørende SIS og VIS bestemmelser, der bygger på eller på anden måde har tilknytning til Schengenreglerne, jf. de respektive tiltrædelsesakter.

Centrale bestemmelser

Forordningen[98] præciserer målene for EES, de kategorier af oplysninger, der skal registreres i EES, de formål, som oplysningerne skal bruges til, kriterierne for registrering af oplysningerne, hvilke myndigheder der skal have adgang til oplysningerne, yderligere regler for databehandling og beskyttelse af personoplysninger samt EES-systemets tekniske arkitektur, bestemmelser om dets drift og brug og dets interoperabilitet med andre informationssystemer. EES sigter mod at forbedre forvaltningen af de ydre grænser, forhindre irregulær indvandring og gøre det lettere at forvalte migrationsstrømme. Med henblik herpå er EES udformet til at registrere og lagre data, tidspunkt og sted for visse tredjelandsstatsborgeres ind- og udrejse ved passage af de af medlemsstaternes grænser, hvor ind- og udrejsesystemet anvendes. Derudover kan de nationale retshåndhævende myndigheder søge i EES med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger[99].

EES består af et centralt system (det centrale EES-system), som anvender en central elektronisk database med biometriske og alfanumeriske oplysninger, en national ensartet grænseflade i hver medlemsstat. En sikker kommunikationskanal forbinder det centrale EES-system med det centrale visuminformationssystem (det centrale VIS-system), og en sikker og krypteret kommunikationsinfrastruktur forbinder det centrale EES-system med den nationale ensartede grænseflade. Interoperabilitet etableres mellem EES og VIS ved hjælp af en direkte kommunikationskanal mellem deres centrale systemer, så grænsemyndighederne kan søge i VIS fra EES, og visummyndighederne kan søge i EES fra VIS.

---

98 Kommissionen bestemmer, fra hvilken dato EES skal idriftsættes, når betingelserne i artikel 66 i forordning (EU) 2017/2226 er opfyldt.

99 Ved "terrorhandling" forstås en lovovertrædelse, der svarer til eller er ligestillet med en af de lovovertrædelser, der er omhandlet i direktiv (EU) 2017/541; ved "alvorlig strafbar handling" forstås en lovovertrædelse, som svarer til eller er ligestillet med en af de i artikel 2, stk. 2, i rammeafgørelse 2002/584/RIA om den europæiske arrestordre omhandlede lovovertrædelser, hvis de i henhold til national ret kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år.

Forordningen fastsætter strenge regler for adgang til EES. Det indeholder også regler om enkeltpersoners ret til indsigt, berigtigelse, supplering, sletning og klageadgang, navnlig retten til domstolsprøvelse og uafhængige offentlige myndigheders tilsyn med behandlingen af oplysningerne.

Forordningen overholder de grundlæggende rettigheder og de principper, der er fastlagt i EU's charter om grundlæggende rettigheder. Uden at dette berører de mere specifikke bestemmelser i forordningen om behandling af personoplysninger, finder forordning (EU) nr. 2016/679[100] ("den generelle forordning om databeskyttelse") anvendelse på behandlingen af personoplysninger under anvendelsen af denne forordning, medmindre en sådan behandling foretages af de udpegede retshåndhævende myndigheder eller centrale adgangspunkter i medlemsstaterne, i hvilke tilfælde direktiv (EU) 2016/680[101] ("politidirektivet") finder anvendelse.

3.20. Europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS)

Lovgivning

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

Europa-Parlamentets og Rådets forordning (EU) 2018/1241 af 12. september 2018 om ændring af forordning (EU) 2016/794 med henblik på oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) (EUT L 236 af 19.9.2018, s. 72).

---

100 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).

101 Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2019 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).

Forordning 2018/1240[102] præciserer målene for ETIAS, fastlægger dets tekniske og organisatoriske opbygning, fastsætter bestemmelser vedrørende drift og brug af de oplysninger, som ansøgeren skal indlæse i systemet, fastsætter bestemmelser for udstedelse af eller afslag på rejsetilladelsen, fastsætter formålet med at behandle oplysningerne, bestemmer, hvilke myndigheder der skal have ret til at få adgang til oplysningerne, og sikrer beskyttelse af personoplysninger.

Forordningen udgør en udvikling af bestemmelser i Schengenreglerne. Det Forenede Kongerige og Irland deltager ikke i gældende EU-ret, og forordningen er derfor ikke bindende for og finder ikke anvendelse i Det Forenede Kongerige og Irland. Gældende EU-ret er bindende for Island, Norge, Liechtenstein og Schweiz i henhold til de respektive aftaler eller protokollen vedrørende Schengenreglerne.

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

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

Centrale bestemmelser

ETIAS giver en rejsetilladelse, der er af en anden karakter end et visum, men som udgør en betingelse for indrejse og ophold i Schengenområdet, og som angiver, at den person, der ansøger om en rejsetilladelse, ikke udgør en risiko for sikkerheden, en risiko for ulovlig indvandring eller en høj risiko for epidemi i Unionen.

ETIAS består af et:

- omfattende informationssystem, dvs. ETIAS-informationssystemet, der er udformet, udviklet og teknisk forvaltet af eu-LISA

[102] Kommissionen bestemmer, fra hvilken dato EES skal idriftsættes, når betingelserne i artikel 88 i forordning (EU) 2018/1240 er opfyldt.

- Den centrale ETIAS-enhed, som er del af Det Europæiske Agentur for Grænse- og Kystbevogtning

- De nationale ETIAS-enheder, ansvarlige for at behandle ansøgninger og afgøre, om de vil udstede eller afvise, annullere eller inddrage rejsetilladelser. Med henblik herpå bør de nationale enheder samarbejde med hinanden og med Europol med henblik på at vurdere ansøgninger.

Adgangen til personoplysninger i ETIAS bør være forbeholdt direkte bemyndiget personale, og adgangen bør under ingen omstændigheder anvendes til at træffe afgørelser baseret på nogen form for forskelsbehandling. Hvad angår retshåndhævende myndigheder, som er udpeget af medlemsstaterne, bør behandling af personoplysninger lagret i det centrale ETIAS-system kun finde sted i særlige tilfælde og kun, når det er nødvendigt med henblik på at forebygge, afsløre eller efterforske terrorhandlinger eller andre alvorlige strafbare handlinger. De udpegede myndigheder og Europol bør kun anmode om adgang til ETIAS, når de har rimelig grund til at antage, at en sådan adgang vil kunne tilvejebringe oplysninger, der kan hjælpe dem med at forebygge, opdage eller efterforske en terrorhandling eller en anden alvorlig strafbar handling.

Forordningen respekterer de grundlæggende rettigheder og overholder de principper, der er anerkendt i Den Europæiske Unions charter om grundlæggende rettigheder. Med hensyn til behandlingen af personoplysninger har de fornødne garantier derfor til formål at begrænse indgrebet i retten til beskyttelse af privatlivets fred og retten til beskyttelse af personoplysninger til, hvad der er nødvendigt og rimeligt i et demokratisk samfund.

Forordning (EU) nr. 2016/679 ("den generelle forordning om databeskyttelse")103 finder anvendelse på behandlingen af personoplysninger under anvendelsen af denne forordning, medmindre en sådan behandling foretages af de udpegede retshåndhævende myndigheder eller centrale adgangspunkter i medlemsstaterne, i hvilke tilfælde direktiv (EU) 2016/680104 ("politidirektivet") finder anvendelse.

---

103 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 (EUT L 119 af 4.5.2016, s. 1).

104 Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2019 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge

3.21. Lovgivningen om interoperabilitet

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

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

Centrale bestemmelser

Forordning (EU) 2019/817 og forordning (EU) 2019/818 udgør "interoperabilitetspakken" og fokuserer på personoplysninger, der lagres i centrale EU-informationssystemer. Forordningerne har til formål at forbedre Unionens dataforvaltningsstruktur for både grænseforvaltning og sikkerhed. Rammerne for "interoperabilitetspakken" finder således anvendelse på behandlingen af personoplysninger i forbindelse med grænser og visum eller politisamarbejde og retligt samarbejde, asyl og migration. Interoperabiliteten mellem disse underliggende informationssystemer bør gøre det muligt for dem at supplere hinanden, så de bedre kan opfylde deres respektive formål. Forordningerne tilpasser også procedurerne og betingelserne for de udpegede myndigheders og Europols adgang til EES, VIS, ETIAS og Eurodac med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger og grov kriminalitet.

De tekniske interoperabilitetskomponenter omfatter EES (se punkt 3.18), VIS (se punkt 3.7), ETIAS (se punkt 3.19), Eurodac (se punkt 3.8), SIS (se punkt 3.2) og ECRIS-TCN (se punkt 3.13.2). Interoperabilitetskomponenterne[105] er:

- Den europæiske søgeportal (ESP), forstået som et enkelt vindue eller en "meddelelsesformidler", der gør det muligt at søge parallelt i de ovennævnte EU-instrumenter, Europoldata og INTERPOL-databaser. Søgningerne er begrænset til oplysninger vedrørende personer eller rejsedokumenter;

---

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).

105 Kommissionen fastsætter den dato, fra hvilken bestemmelserne i forordningerne vedrørende ESP, den fælles biometriske matchtjeneste, det fælles identitetsregister og multiidentitetsdetektoren finder anvendelse.

- den fælles biometriske matchtjeneste (fælles BMS), hvis hovedformål er at gøre det lettere at identificere en person, der er registreret i flere databaser, ved at anvende en enkelt teknologisk komponent, der matcher vedkommendes biometriske data på tværs af forskellige systemer. De AFIS-skabeloner, der anvendes, bør samles og lagres i BMS på ét enkelt sted;

- et fælles identitetsregister, forstået som et fælles register for identitetsdata, rejsedokumenter og biometriske data for personer, der er registreret i EES, VIS, ETIAS, Eurodac og ECRIS-TCN. Disse oplysninger kan vedrøre den samme person, men under forskellige eller ufuldstændige identiteter. Der bør opnås større nøjagtighed i identifikationen ved hjælp af en automatiseret sammenligning og matchning af oplysningerne. Det fælles identitetsregister giver de udpegede retshåndhævende myndigheder mulighed for at foretage identitetskontrol med henblik på at støtte deres bestræbelser på at identificere en person;

- multiidentitetsdetektoren (MID), som understøtter det fælles identitetsregister.

De nye behandlinger af oplysninger, der er fastsat i forordningerne, griber ind i de grundlæggende rettigheder, der er beskyttet ved artikel 7 og 8 i EU's charter om grundlæggende rettigheder. Eftersom en effektiv gennemførelse af EU-informationssystemerne afhænger af, at der foretages en korrekt identifikation af den pågældende person, er et sådant indgreb i tråd med de samme mål, som hvert af disse systemer er blevet oprettet for, nemlig effektiv forvaltning af Unionens grænser, den interne sikkerhed i Unionen, effektiv gennemførelse af Unionens asyl- og visumpolitik.

Forordning (EU) 2016/679 finder anvendelse på behandling af personoplysninger med henblik på interoperabilitet, medmindre en sådan behandling foretages af de udpegede retshåndhævende myndigheder eller centrale adgangspunkter i medlemsstaterne med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger. I dette tilfælde finder direktiv (EU) 2016/680 (se punkt 3) anvendelse.

De tilsynsmyndigheder, der er omhandlet i forordning (EU) 2016/679 eller direktiv (EU) 2016/680, bør kontrollere, at medlemsstaternes behandling af personoplysninger er lovlig. Den Europæiske Tilsynsførende for Databeskyttelse bør overvåge EU-institutionernes og -organernes aktiviteter i forbindelse med behandling af personoplysninger.