EUROPA-
KOMMISSIONEN

Bruxelles, den 7.12.2012
COM(2012) 735 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Styrkelse af samarbejdet om retshåndhævelse i EU: den europæiske informationsudvekslingsmodel (EIXM)

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Styrkelse af samarbejdet om retshåndhævelse i EU: den europæiske informationsudvekslingsmodel (EIXM)

1. INDLEDNING

Sikring af et højt sikkerhedsniveau i EU og Schengenområdet kræver, at der sættes ind over for kriminelle netværk via en fælles indsats på EU-plan[1]. Det er nødvendigt at tage fat om ikke kun alvorlig og organiseret kriminalitet, som f.eks. menneskehandel, ulovlig narkotikahandel og ulovlig våbenhandel, men også mindre alvorlige overtrædelser, der i stort omfang begås af mobile organiserede kriminelle grupper, og kriminalitet, der begås af individuelle lovovertrædere på tværs af medlemsstaternes grænser.

Udveksling af oplysninger mellem medlemsstaterne er i denne sammenhæng et afgørende redskab for de retshåndhævende myndigheder. Internationale og bilaterale ordninger er derfor blevet suppleret af EU-instrumenter og -systemer, som f.eks. Schengeninformationssystemet og Europols informationssystem, med indbyggede foranstaltninger til beskyttelse af privatlivets fred og personoplysninger i overensstemmelse med chartret om grundlæggende rettigheder. Denne meddelelse gør status over, **hvordan** den resulterende **grænseoverskridende informationsudveksling i EU fungerer i dag**, og indeholder anbefalinger til, hvordan den kan forbedres.

Den konkluderer, at informationsudvekslingen generelt fungerer godt, og der gives i det følgende eksempler på vellykkede resultater, der illustrerer dette. **Der er derfor ikke behov for nye retshåndhævelsesdatabaser eller instrumenter til informationsudveksling på EU-plan på nuværende tidspunkt**. De eksisterende EU-instrumenter kan og bør dog anvendes mere effektivt, og udvekslingen bør organiseres på en mere ensartet måde.

Denne meddelelse indeholder derfor anbefalinger til medlemsstaterne om, hvordan de kan **forbedre gennemførelsen af de eksisterende instrumenter** og **strømline de anvendte kommunikationskanaler**. Den understreger behovet for at **sikre høj datakvalitet, -sikkerhed og -beskyttelse**. Den beskriver også, hvordan Kommissionen vil støtte medlemsstaternes indsats, herunder via **finansiering og uddannelse**. På den måde leverer den en model for retningslinjer vedrørende EU's og medlemsstaternes aktiviteter.

Denne meddelelse imødekommer opfordringen i Stockholmprogrammet til Kommissionen om at vurdere behovet for en europæisk informationsudvekslingsmodel baseret på en evaluering af de eksisterende instrumenter. Den bygger videre på Kommissionens meddelelse fra 2010 "Oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed"[2] og på EU's informationsstyringsstrategi for intern sikkerhed, som blev godkendt i 2009[3], samt de foranstaltninger, som medlemsstaterne, Kommissionen og Europol har iværksat for at gennemføre den ("IMS-foranstaltningerne"). Den støtter sig også til en kortlægning af EU's

[1] Strategien for EU's indre sikkerhed i praksis, KOM(2010) 673.
[2] KOM(2010) 385.
[3] Rådets konklusioner 16637/09 af 30. november 2009.

informationsudveksling, som involverer nationale og andre eksperter (EDPS, EU-agenturer og Interpol), en undersøgelse af informationsudveksling mellem retshåndhævende myndigheder[4] og drøftelser med aktører, herunder databeskyttelsesmyndigheder.

2. DEN NUVÆRENDE SITUATION

De retshåndhævende myndigheder udveksler oplysninger til forskellige formål, bl.a. med henblik på strafferetlig efterforskning, kriminalitetsforebyggelse, opklaring af kriminalitet (f.eks. ved hjælp af kriminalefterretningsoperationer) og sikring af offentlig orden og sikkerhed. Hvad angår omfanget af grænseoverskridende udveksling, viste ovennævnte undersøgelse fra 2010, som omfattede svar fra nationale agenturer i medlemsstaterne, at omkring en fjerdedel af deres anmodninger om efterforskning og kriminalefterretningsoperationer blev sendt til andre EU-lande eller Schengenlande.

2.1. Instrumenter

Kommissionens oversigt over informationsstyring fra 2010 beskriver alle instrumenter på EU-niveau, som regulerer indsamling, lagring og grænseoverskridende udveksling af personoplysninger med henblik på retshåndhævelse eller migrationsforvaltning. Denne meddelelse fokuserer på de **instrumenter, der anvendes til grænseoverskridende udveksling mellem medlemsstaterne**. Medlemsstaterne har fremlagt eksempler på, hvordan disse instrumenter anvendes.

Det svenske initiativ[5] fastlægger regler, herunder tidsfrister, for udveksling af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder til brug i strafferetlig efterforskning eller kriminalefterretningsoperationer. Det bygger på princippet om "lige adgang", dvs. at betingelserne for udlevering af oplysninger til anmodende medlemsstater ikke må være mere restriktive end de betingelser, der gælder nationalt. Oplysninger skal også udveksles med Europol og Eurojust, hvis udvekslingen vedrører overtrædelser inden for deres mandat.

I 2012 snød en velkendt italiensk svindler en svensk virksomhed til at indbetale 65 000 EUR på en italiensk konto. Det svenske SPOC (se punkt 3.2 nedenfor) modtog en anmodning fra Italien via Sirene-kanalen (se nedenfor) om at forespørge virksomhedens direktør, om betalingen var blevet foretaget, i hvilket tilfælde Italien ville fastfryse pengene. Sverige iværksatte foranstaltninger og svarede i henhold til det svenske initiativ inden for mindre end 24 timer. Takket være denne hurtige indsats modtog det svenske politi oplysninger om, at en virksomhed var offer for svindel, og de italienske myndigheder modtog de oplysninger, de skulle bruge for at kunne gribe ind, og pengene vil sandsynligvis blive tilbagebetalt.

I 2012 gav en belgiskfødt mand på skadestuen på et hospital i nærheden af Paris en forvirret redegørelse for, hvordan han var blevet påført et alvorligt skudsår. Hans ledsagers udtalelser fik efterforskerne til at undersøge mulige begivenheder i Belgien. De første forespørgsler afslørede, at manden var kendt i Belgien, herunder for mord. Under det svenske initiativ sendte de franske myndigheder spontane oplysninger til det belgiske politi, der hurtigt sammenkædede dem med begivenheder to dage tidligere i Belgien, hvor fire bevæbnede mænd kidnappede en medarbejder i en guldsmedeforretning. Politiets indsats havde fået mændene til at flygte. Mændene undslap, men den ene blev ramt i en skududveksling med politiet. Disse

[4] http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm.

[5] Rådets rammeafgørelse 2006/960/RIA.

oplysninger fik de franske myndigheder til at anbringe manden under opsyn, indtil der blev udstedt en europæisk arrestordre, som blev udstedt samme dag i Belgien og overført til Frankrig via Sirene.

Prümafgørelsen[6] omhandler automatisk udveksling af dna-profiler, fingeraftryksoplysninger og oplysninger i køretøjsregistre med henblik på at efterforske forbrydelser (for dna, fingeraftryksoplysninger og oplysninger i køretøjsregistre), forebygge forbrydelser (fingeraftryksoplysninger og oplysninger i køretøjsregistre) og sikre den offentlige orden (oplysninger i køretøjsregistre). Sammenligning af biometriske data (dna og fingeraftryk) fungerer som et system med "hit/ikke-hit", hvor en automatisk sammenligning producerer et anonymt "hit", hvis de dna- eller fingeraftryksoplysninger, som den anmodende medlemsstat har registreret, matcher data, som en anden medlemsstat har registreret. De tilknyttede person- eller sagsoplysninger udleveres kun efter en separat opfølgende anmodning.

En mand blev fundet knivdræbt i en lejlighed i en tysk by. Der blev fundet et fingeraftryk på en dørkarm. En automatisk Prümsøgning gav et hit i den bulgarske database. Opfølgende oplysninger, som Bulgarien blev anmodet om, blev fremsendt inden for tre timer og straks indtastet i Schengeninformationssystemet (SIS – se nedenfor). Næste dag blev den pågældende person arresteret i Østrig.

I 2007, da Prümudvekslinger lige var blevet indført, blev der stjålet udstyr fra en politibil i Wien. Et dna-spor fra bilen blev matchet i den østrigske database med et spor fra en tilsvarende sag, men det var et Prüm-hit i den tyske database, der førte til identifikationen af en polsk serieindbrudstyv. En europæisk arrestordre blev udstedt i Østrig. Den mistænkte blev arresteret i Polen (takket være et hit i en SIS-indberetning) og blev senere dømt i Østrig.

Europol støtter medlemsstaternes indsats og samarbejde i bestræbelserne på at forebygge og bekæmpe organiseret kriminalitet, terror og andre former for alvorlig kriminalitet (jf. bilaget til Rådets afgørelse om Europol[7]), som berører to eller flere medlemsstater. Det tilvejebringer en platform, hvor medlemsstaterne – via Europols nationale enheder – kan udveksle strafferetlige efterretninger og oplysninger. Europols informationssystem er en database med oplysninger (183 000 elementer), som medlemsstaterne har indgivet om grænseoverskridende kriminalitet inden for Europols mandat, navne på implicerede personer (41 000) og andre relaterede data. Europol bruger databasen til sine analyser, og medlemsstaterne kan bruge den til efterforskningsformål. Siden 2011 har medlemsstaterne kunnet give andre retshåndhævende myndigheder end Europols nationale enheder adgang til at foretage søgninger med "hit/ikke-hit". Analysedatabasen sætter Europol i stand til at levere operationelle analyser til støtte for grænseoverskridende efterforskninger.

Forfalskede betalingskort blev anvendt til at hæve store beløb fra kontantautomater forskellige steder i Slovenien. To bulgarske borgere blev efterforsket. Brugen af Europols informationssystem (EIS) førte til et hit, der viste, at den ene af dem havde begået lignende handlinger i Frankrig og Italien. Frankrig indgav detaljerede oplysninger til EIS. Takket være et hurtigt svar fra Frankrig via SIENA (se nedenfor) efterfulgt af en fingeraftrykskontrol og ophævelse af en begrænsning for håndteringen kunne de slovenske myndigheder bruge dataene som bevis i retssagen. Europols analysedatabase påviste forbindelser mellem sager i SI, BG, FR, IE, IT og NO.

[6] Rådets afgørelse 2008/615/RIA.

[7] 2009/371/RIA.

Schengeninformationssystemet (SIS) indeholder indberetninger om personer og genstande. Som kompenserende foranstaltning for ophævelsen af grænsekontrollen ved de indre grænser anvendes det både inden for Schengenområdet og ved dets ydre grænser med henblik på at opretholde et højt sikkerhedsniveau i området. Det er et omfattende system (over 43 mio. indberetninger), som personalet i marken kan bruge til at foretage hit/ikke-hit-søgninger. Efter et hit (hvis f.eks. detaljer om en person eller en genstand matcher en indberetning) kan der indhentes supplerende oplysninger via Sirene-kontorerne (se nedenfor). SIS vil blive erstattet af **SIS II**, der indeholder en række forbedringer, som f.eks. mulighed for at sammenkæde relaterede indberetninger (f.eks. indberetning om en person og et køretøj), nye kategorier af indberetninger og en funktion til lagring af fingeraftryk, fotos og kopier af europæiske arrestordrer. Rådets afgørelse om SIS II[8] definerer kategorier af underretninger til støtte for samarbejdet mellem politiet og retsmyndighederne i kriminalsager. I den forbindelse deltager alle EU-medlemsstater i SIS II, mens Europol og Eurojust fortsat har adgang. Forvaltningen af centrale elementer af SIS II vil blive overdraget til It-Agenturet[9].

Andre EU-instrumenter eller it-systemer støtter udvekslingen af oplysninger vedrørende retshåndhævelse mellem toldmyndighederne (Napoli II-konventionen, toldinformationssystemet, som er en del af de AFIS-databaser, der drives af Det Europæiske Kontor for Bekæmpelse af Svig – OLAF), finansielle efterretningsenheder, kontorer for inddrivelse af aktiver og platforme for indberetning af it-kriminalitet[10]. Bestemmelser om retshåndhævende myndigheders adgang til andre omfattende EU-systemer er indført (visuminformationssystemet) eller foreslået (Eurodac[11]) med henblik på at forebygge, opdage og efterforske terror og anden alvorlig kriminalitet. Spørgsmålet om, hvorvidt retshåndhævende myndigheder skal have adgang og i givet fald på visse betingelser, indgår også i det forberedende arbejde, der i øjeblikket pågår i forbindelse med det forslag til et ind- og udrejsesystem, som ventes fremlagt inden længe.

Der udvikles et europæisk grænseovervågningssystem (Eurosur) med henblik på informationsudveksling og operationelt samarbejde mellem nationale koordinationscentre og med Frontex med det formål at forbedre deres overblik over situationen og mulighed for hurtige indgreb, således at ulovlig indvandring og grænseoverskridende kriminalitet kan forhindres ved EU's ydre grænser. En fælles ramme for informationsudveksling med henblik på overvågning af EU's maritime område, som bl.a. har til formål at sikre et klart overblik over situationen til søs, udvikles med henblik på at muliggøre udveksling af oplysninger mellem offentlige myndigheder i syv relevante sektorer (herunder generelle retshåndhævelsesorganer) og på tværs af grænser, samtidig med at interoperabiliteten mellem eksisterende og fremtidige overvågningssystemer, som f.eks. Eurosur, bevares.

Medlemsstaterne udveksler også oplysninger i medfør af nationale love og bilaterale aftaler. De er også alle medlemmer af Interpol, hvorigennem oplysninger kan udveksles med lande i hele verden via enten Interpol-meddelelser og -databaser (f.eks. databaser over stjålne og bortkomne rejsedokumenter) eller bilateralt ved hjælp af Interpol-kanalen.

---

8 2007/533/RIA.

9 Det Europæiske Agentur for den Operationelle Forvaltning af Store It-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed.

10 Den kommende europæiske strategi for internetsikkerhed repræsenterer en anledning til at vurdere de fremtidige behov for informationsudveksling mellem net- og informationssikkerhedsmyndighederne og de retshåndhævende myndigheder, f.eks. via det europæiske center til bekæmpelse af it-kriminalitet.

11 EU-database over fingeraftryk fra asylansøgere og andre, der krydser grænserne ulovligt.

2.2. Kanaler og kommunikationsværktøjer

Der anvendes **tre hovedkanaler** til grænseoverskridende udveksling af oplysninger, som hver især er baseret på nationale enheder i hver medlemsstat, der anvender et tilknyttet kommunikationsværktøj:

(1) **Sirene**[12]-kontorerne kan efter et hit i en SIS-indberetning indhente supplerende oplysninger fra den medlemsstat, der har indgivet indberetningen. De arbejder døgnet rundt og følger procedurerne i Sirene-håndbogen. I øjeblikket udveksler de oplysninger via Sisnet-systemet, som vil blive erstattet af SIS II-kommunikationsnettet ved udgangen af marts 2013.

(2) **Europols** nationale enheder udveksler oplysninger med Europol. De udveksler i nogle tilfælde også oplysninger bilateralt om kriminalitet uden for Europols mandat og uden at inddrage Europol. Europols nationale enheder kan udveksle oplysninger direkte eller via Europol-forbindelsesofficerer, der er en del af en national enhed, men som er udstationeret i Europols hovedkvarter. Europol har udviklet et sikkert kommunikationsværktøj, **SIENA**[13], til udveksling af oplysninger med Europol og mellem medlemsstaterne. I 2011 anvendte medlemsstaterne SIENA til at udveksle 222 000 meddelelser. I 53 % af tilfældene blev oplysningerne i meddelelserne delt med Europol.

(3) **Interpols** nationale centrale bureauer, som arbejder døgnet rundt, udveksler oplysninger med Interpol og bilateralt uden at involvere Interpol. De nationale centrale bureauer bruger kommunikationsværktøjet I-24/7, som er udviklet af Interpol.

Andre kanaler omfatter bilaterale forbindelsesofficerer (som er udstationeret i andre medlemsstater og typisk anvendes i mere komplicerede sager) og politi- og toldsamarbejdscentre (etableret af nabomedlemsstater med henblik på at støtte informationsudvekslingen og det operationelle samarbejde i grænseområder).

Valget af kanal er delvist reguleret af EU-lovgivningen. SIS-anmodninger om supplerende oplysninger efter et hit skal sendes via Sirene-kontorerne, og informationsudveksling med Europol skal ske via de nationale enheder. I andre tilfælde vælges kanalen af medlemsstaten.

2.3. Samspil mellem instrumenter, kanaler og værktøjer

Der er en række forskellige instrumenter, kanaler og værktøjer, som hver især er udviklet til et særligt formål. En strafferetlig efterforskning kan involvere parallel eller sekventiel brug af mere end et instrument. I en grænseoverskridende sag med alvorlig eller organiseret kriminalitet kan en person eller en genstand kontrolleres i både Europols informationssystem og SIS, og hvis der er "hits", kan opfølgende anmodninger sendes via henholdsvis Europol eller Sirene. Et biometrisk spor kan være genstand for en Prümudveksling, som efter et hit efterfølges af en anmodning, der sendes ved hjælp af SIENA-værktøjet i medfør af det svenske initiativ.

---

[12] **S**upplementary **I**nformation **RE**quest at the **N**ational **E**ntry (anmodning om supplerende oplysninger ved det nationale grænseovergangssted).

[13] **S**ecure **I**nformation **E**xchange **N**etwork **A**pplication.

Uanset kombinationen eller sekvensen skal reglerne for hvert enkelt instrument overholdes. De omfatter regler om databeskyttelse, om datasikkerhed og -kvalitet og om det formål, som instrumenter må anvendes til. National behandling af data til grænseoverskridende udveksling skal også være i overensstemmelse med EU's lovgivning om beskyttelse af personoplysninger[14]. Proportionalitetsprincippet skal overholdes. Anmodninger kan f.eks. afvises i henhold til det svenske initiativ, hvis videregivelse af oplysningerne vil stå i klart misforhold til formålet med anmodningen. Overholdelse af disse regler kræver, at anmodninger og svar kontrolleres af kvalificerede medarbejder, som benytter hensigtsmæssige informationsværktøjer.

2.4. Grænseflade med retligt samarbejde

Den strafferetlige proces involverer både retshåndhævende myndigheder og retlige myndigheder, men forskelle mellem medlemsstaterne omfatter det omfang, hvori de retlige myndigheder (herunder anklagere) leder eller fører tilsyn med den strafferetlige efterforskning. Hvis efterforskning ledes af de retlige myndigheder, og hvis oplysninger skal bruges som bevismateriale, kræves der typisk retlige samarbejdsprocedurer med gensidig retshjælp.

Oplysninger, der er direkte tilgængelige for de retshåndhævende myndigheder i en medlemsstat, kan desuden kræve tilladelse fra de retlige myndigheder i en anden. Hvis de ønskede oplysninger kræver tilladelse fra de retlige myndigheder, skal den adspurgte retshåndhævende myndighed i henhold til det svenske initiativ forespørge de retlige myndigheder, som skal anvende de samme regler som i en rent national sag.

I henhold til kortlægningen vurderer eksperter i retshåndhævelse dog, at de forskellige regler forårsager forsinkelser i grænseoverskridende efterforskninger. Selv om det er uden for anvendelsesområdet for denne meddelelse, bemærkes det, at Eurojust kan lette det retlige samarbejde. Det er også relevant at nævne den europæiske efterforskningskendelse, som i øjeblikket forhandles, og som vil erstatte de eksisterende regler om grænseoverskridende indsamling af bevismateriale og gennemføre princippet om gensidig anerkendelse. Det vil blive krævet, at den anerkendes og gennemføres med samme hast som en tilsvarende national sag og under alle omstændigheder inden for de angivne tidsfrister.

2.5. Principper

I sin oversigt over informationsstyring fra 2010 fastlagde Kommissionen materielle og procesorienterede principper for udviklingen af nye initiativer og evaluering af nuværende instrumenter.

De materielle principper er:

(1) *Beskytte de grundlæggende rettigheder, navnlig retten til respekt for privatliv og beskyttelse af personoplysninger.* Disse er rettigheder i henhold til artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 16 i traktaten om Den Europæiske Unions funktionsmåde.

(2) *Nødvendighed.* En begrænsning af retten til respekt for privatliv kan kun begrundes, hvis den er lovlig, har et lovligt formål og er nødvendig i et demokratisk samfund.

[14] Rådets rammeafgørelse 2008/977/RIA.

(3) *Nærhedsprincippet*.

(4) *Præcis risikostyring.* Nødvendige undersøgelser og nødvendig formålsbegrænsning har afgørende betydning.

De procesorienterede principper er:

(5) *Omkostningseffektivitet.* Dette kræver, at der tages højde for allerede eksisterende løsninger, og at det vurderes, om et forslags målsætninger kan opfyldes gennem en bedre brug af allerede eksisterende instrumenter.

(6) *Bottom-up-politikudformning* Et eksempel på dette er kortlægningen i forbindelse med udarbejdelsen af denne meddelelse, som involverede eksperter i retshåndhævelse.

(7) *Klar ansvarsfordeling.* I oversigten over informationsstyring fra 2010 bemærkes det, at medlemsstaterne ikke har en projektleder at henvende sig til for at få råd om gennemførelsen af Prümafgørelsen. Kommissionens Prümrapport bemærker, hvordan denne mangel i dag delvist afhjælpes med støtte fra Europol. Med hensyn til idéen i oversigten over informationsstyring fra 2010 om, at It-Agenturet kan yde teknisk rådgivning, er dette ikke i centrum for agenturets nuværende prioriteter. Dette kan genovervejes i forbindelse med den treårige evaluering, der skal gennemføres ved udgangen af 2015.

(8) *Bestemmelser om revision og ophør*. Kommissionen har udsendt rapporter om det svenske initiativ og Prüm. Denne meddelelse tager højde for disse.

3. VURDERING OG ANBEFALINGER

Dette afsnit fokuserer på det svenske initiativ, Prüm og Europol-kanalen. Selv om SIS og Sirene-kanalen tegner sig for en stor del af informationsudvekslingen, gives der ikke her anbefalinger vedrørende disse, fordi betydelige ændringer allerede er i støbeskeen, herunder den kommende overgang til SIS II.

3.1. Forbedret brug af eksisterende instrumenter

Ud over den kommende Europol-reform agter Kommissionen ikke på kort sigt at foreslå ændringer af ovennævnte EU-instrumenter. Der er heller ikke brug for nye instrumenter på nuværende tidspunkt. Først og fremmest skal de **eksisterende instrumenter gennemføres**.

Dette gælder især for Prüm. I Kommissionens Prümrapport, som ledsager denne meddelelse, konkluderes det, at dataudveksling i henhold til Prüm i høj grad er nyttig i forbindelse med efterforskning, men gennemførelsen er alvorligt bagud. **Mange medlemsstater udveksler ikke data i henhold til Prüm, selv om fristen for gennemførelse var den 26. august 2011**[15]. Hovedårsagerne er af teknisk karakter og skyldes mangel på menneskelige og finansielle ressourcer i medlemsstaterne. I betragtning af mulighederne for EU-støtte

[15] Følgende medlemsstater har gennemført:
DNA: BG/CZ/DE/ES/EE/FR/CY/LV/LT/LU/HU/NL/AT/PT/RO/SI/SK/FI;
FP: BG/CZ/DE/EE/ES/FR/CY/LT/LU/HU/NL/AT/SI/SK;
VRD: BE/DE/ES/FR/LT/LU/NL/AT/PL/RO/SI/FI/SE.
Yderligere oplysninger findes i Prümrapporten.

(finansiering, mobilt kompetenceteam og helpdesk) mangler der dog tilsyneladende først og fremmest politisk vilje til at gennemføre afgørelsen. Som anført i rapporten vil Kommissionen fortsat bidrage med tilbud om EU-finansiering. Konteksten vil dog ændre sig i december 2014, når Kommissionen kan indlede overtrædelsesprocedurer. Reglerne om kontrol af den nationale gennemførelse træder først i kraft på det tidspunkt, da Prüm ligesom det svenske initiativ blev vedtaget under den tidligere tredje søjle.

Hvad angår **det svenske initiativ**, rapporterede Kommissionen i 2011, at instrumentet endnu ikke havde nået sit fulde potentiale, men at dets betydning ville stige[16]. Denne vurdering gælder stadig. Ikke alle medlemsstater har gennemført initiativet[17]. De fleste medlemsstater har meddelt, at de har gennemført det i deres nationale lovgivning[18], mens nogle har meddelt, at de ikke behøver gennemføre initiativet, da deres nationale lovgivning allerede er i overensstemmelse hermed[19]. Trods dets fordele, herunder princippet om lige adgang og tidsfrister, er dets praksis stadig ikke udbredt. Som årsag angives det bl.a., at alternativer vurderes at være tilstrækkelige, og at anmodningsformularen er besværlig (selv i den forenklede version fra 2010[20]).

Kommissionen blev anmodet om at undersøge initiativets anvendelighed i forbindelse med opfølgningsanmodninger efter hits i henhold til Prüm[21]. Når opfølgende oplysninger skal bruges som bevismateriale i retten, kræves der normalt en anmodning om retligt samarbejde. Hvis brug som bevismateriale ikke er påkrævet eller endnu ikke er påkrævet, bør systematisk anvendelse af det svenske initiativ som retsgrundlag og SIENA som kommunikationsværktøj fremmes med henblik på fuldt ud at udnytte fordelene ved begge instrumenter og indføre en fælles bedste praksis i medlemsstaterne.

Hvad angår **Europol**, bekræftede en evaluering i 2012[22] bl.a., at medlemsstaterne ikke i tilstrækkelig grad deler oplysninger med Europol (og dermed med hinanden). Kommissionen vil behandle dette i et forslag om ændring af Europols retsgrundlag. Rådet har opfordret medlemsstaterne til i højere grad at anvende Europols informationssystem[23].

I overensstemmelse med Stockholmprogrammet bestilte Kommissionen en undersøgelse om et muligt **europæisk informationssystem vedrørende strafferegistre**[24]. Hensigten er at imødekomme behovet for, at politiet i én medlemsstat ved, om en mistænkt er kendt af politiet i en anden – et behov, der er opstået som følge af kriminalitetens stadig mere grænseoverskridende karakter. I overensstemmelse med princippet om omkostningseffektivitet vurderer Kommissionen, at det i øjeblikket **ikke kan begrundes** at oprette et europæisk informationssystem vedrørende strafferegistre, når de eksisterende instrumenter og værktøjer, der kunne opfylde dette formål helt eller delvist gennem bedre eller intensiveret udnyttelse, ikke udnyttes fuldt ud. Dette gælder navnlig Europols informationssystem (overførsel af relevante data og udvidet adgang på nationalt plan), SIS II (øget brug af relevante indberetninger af personer eller køretøjer til kontrol med henblik på at retsforfølge straffeovertrædelser og forhindre trusler mod den offentlige sikkerhed), SIENA (videreudvikling af adgang på nationalt plan, sammenkædning med nationale systemer og

16 SEK(2011) 593.
17 Følgende medlemsstater mangler stadig at vedtage gennemførelseslovgivning: BE/EL/IT/LU.
18 BG/CZ/DK/DE/EE/ES/FR/CY/HU/LT/LV/NL/PL/PT/RO/SI/SK/FI/SE.
19 IE/MT/AT/UK.
20 9512/1/10.
21 Rådets konklusioner 15277/11 af 27.-28. oktober 2011.
22 https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf.
23 Rådets konklusioner af 7.-8. juni 2012.
24 http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm.

automatisering af opgaver efter behov) og Prüm (fuld gennemførelse med henblik på at forbedre identifikationen af kriminelle, der opererer i forskellige medlemsstater).

Medlemsstaterne opfordres til

- fuldt ud at gennemføre det svenske initiativ, herunder dets princip om lige adgang
- fuldt ud at gennemføre Prümafgørelsen ved hjælp af den tilgængelige EU-støtte
- for opfølgningsanmodninger efter hits i henhold til Prüm at bruge det svenske initiativ og SIENA-værktøjet.

Kommissionen vil

- fortsat yde EU-finansiering til støtte for gennemførelsen af Prüm
- inden december 2014 forberede anvendelsen af reglerne om kontrol med den nationale gennemførelse af EU-lovgivning på dette område.

3.2. Strømlining og forvaltning af kanalerne

Valg af kanal. Et resultat af, at medlemsstaterne frit kan vælge kanal (bortset fra de retlige krav vedrørende Sirene-kontorer og Europols nationale enheder), er, at de bruger forskellige kanaler i forskellige udstrækninger. I 2008 blev der udarbejdet en håndbog med god praksis vedrørende politienheders internationale samarbejde på nationalt plan ("*Manual of Good Practices concerning International Police Cooperation Units at National Level*")[25] under de europæiske politichefer. Denne håndbog indeholder kriterier[26], men de er ikke bindende, og de har ikke resulteret i en samordning af national praksis. Nogle medlemsstater er begyndt at anvende Europol-kanalen mere systematisk. Andre anvender stadig i vid udtrækning Interpol-kanalen, som tilsyneladende foretrækkes, fordi den traditionelt har indgået i det internationale politisamarbejde og angiveligt er let at bruge. Sisnet anvendes af nogle medlemsstater i forbindelse med forhold, der ikke vedrører SIS, f.eks. anmodninger i henhold til det svenske initiativ.

Kommissionen mener, at EU nu bør benytte en mere sammenhængende tilgang, hvor Europol-kanalen spiller en central rolle. Ved denne tilgang, hvor kanalen ikke er defineret i retsgrundlaget, **bør Europol-kanalen baseret på SIENA-værktøjet være standardkanalen**, medmindre der er specifikke grunde til at anvende et andet instrument. Anmodninger om politisamarbejde, der i øjeblikket fremsættes ved hjælp af Sisnet (som lukkes, når SIS II tages i brug[27]), bør i fremtiden fremsættes ved hjælp af SIENA.

Nogle medlemsstater foretrækker en tilgang, der giver bred fleksibilitet til at anvende forskellige kanaler. Kommissionen er uenig i dette. En situation, hvor alle medlemsstater udvikler nationale regler for valget af kanal, og hvor de sikrer samordning mod en fælles tilgang, ville være bedre end den nuværende spredte tilgang. Valget af Europol-kanalen kan begrundes ved dens fordele. Europol-forbindelsesofficerer kan blive anmodet om assistance, når det er nødvendigt. SIENA kan bruges til direkte bilaterale udvekslinger, men fremmer også deling af oplysninger med Europol i overensstemmelse med kravene i Europol-

[25] 7968/08.

[26] Gentaget i retningslinjerne for gennemførelsen af det svenske initiativ, 9512/1/10.

[27] SIS II-kommunikationsnettet er retligt begrænset til SIS II-data og supplerende oplysninger.

afgørelsen og det svenske initiativ. SIENA-meddelelser er trunkerede, kan håndtere store datamængder og udveksles med et højt sikkerhedsniveau. Databeskyttelsen styrkes, når oplysninger udveksles i et struktureret format, f.eks. ved hjælp af SIENA. Den foreslåede tilgang er fuldt ud i overensstemmelse med Kommissionens kommende forslag til en Europol-reform og med Rådets strategiske retningslinjer i Stockholmprogrammet, som angiver, at "Europol bør blive et knudepunkt for informationsudveksling mellem medlemsstaternes retshåndhævende myndigheder, en tjenesteudbyder og en platform for de retshåndhævende tjenester".

Forvaltning af kanalerne. Et SPOC (Single Point of Contact) er en døgnåben kvikskranke for internationalt politisamarbejde, hvor en medlemsstat samler sit Sirene-kontor, sin nationale Europol-enhed og sit nationale Interpol-bureau samt kontaktpunkter for andre kanaler. Hver medlemsstats oprettelse af et SPOC (selv om den term ikke altid er blevet anvendt) var i 2007 en konklusion af den tredje runde af gensidige evalueringsbesøg[28] og anbefales i håndbogen fra 2008. De fleste medlemsstater har afdelinger for internationalt politisamarbejde, men kun nogle af disse kan betegnes som egentlige SPOC'er. I 2012 opfordrede Rådet medlemsstaterne til at undersøge mulighederne for at etablere et SPOC[29]. Kommissionen ønsker at gå videre og mener, at **alle medlemsstater bør etablere SPOC'er** med visse minimumsfunktioner, således at informationsudvekslingen mellem de retshåndhævende myndigheder forbedres som helhed.

Hvis de forskellige kanaler med hensyn til anmodninger til andre medlemsstater samles i én organisatorisk struktur, der er i overensstemmelse med medlemsstatens regler for valg af kanaler, vil det sikre korrekt og konsekvent valg af kanal, og det vil sikre kvaliteten af anmodninger. Kvaliteten sikres, idet SPOC'er validerer anmodninger og bekræfter, at de er nødvendige og hensigtsmæssige. Hvis oplysninger ikke udveksles via et SPOC (f.eks. via politi- og toldsamarbejdscentre (PCCC'er) eller via nationale myndigheder, der foretager direkte udvekslinger ved hjælp af SIENA), kan et SPOC sikre national koordinering. For modtagne anmodninger bør SPOC'er, hvis det tillades i henhold til reglerne, have direkte adgang til nationale databaser, så de hurtigt kan besvare anmodningerne, navnlig inden for tidsfristerne i det svenske initiativ. Reglerne i Sirene-håndbogen (f.eks. om sikkerhed, arbejdsgange, datakvalitet og bemanding) kan bruges som udgangspunkt, således at alle kanaler organiseres på en ensartet måde. Deling af ressourcer, f.eks. personale og infrastruktur, kan bidrage til omkostningsbesparelser eller i det mindste bedre udnyttelse af ressourcerne.

SPOC'er bør omfatte alle retshåndhævende myndigheder, herunder toldmyndigheder. Der bør etableres et samarbejde mellem SPOC'er og nationale koordinationscentre om grænseovervågning. Hvis det er foreneligt med de nationale retssystemer, bør der oprettes forbindelser med retsmyndighederne, især når de fører tilsyn med strafferetlige efterforskninger.

Et stigende antal PCCC'er[30] udveksler oplysninger på lokalt og regionalt plan med godt resultat. Afholdelsen af årlige konferencer på EU-plan sikrer, at der kan udveksles erfaringer, og at fælles tilgange kan drøftes. Selv om det generelt højere antal udvekslinger oftest ikke vedrører den mest alvorlige og organiserede kriminalitet, er det en udfordring at sikre, at oplysninger i relevante tilfælde formidles til nationalt niveau (via SPOC) og til Europol, hvis

[28] 13321/3/07.
[29] Rådets konklusioner 10333/12 af 7.-8. juni 2012.
[30] 38 ved udgangen af 2011.

det er hensigtsmæssigt. I den sammenhæng ser Kommissionen frem til resultaterne af et igangværende pilotprojekt (under en IMS-foranstaltning), hvor SIENA anvendes i et PCCC.

Information Exchange Platform (platform til informationsudveksling) er en IMS-foranstaltning, der ledes af Europol, og som har til formål at udvikle en fælles portal, som giver adgang til eksisterende kanaler og systemer i overensstemmelse med deres regler for sikkerhed og databeskyttelse. Kommissionen vurderer, at der kan opnås fordele ved at gøre brugen af eksisterende kanaler og systemer lettere, men at der er behov for en yderligere vurdering af omkostningerne/fordelene ved en platform til informationsudveksling, hvem der yder finansieringen, og hvordan projektet skal forvaltes. Denne vurdering bør også inddrage It-Agenturet[31].

Medlemsstaterne opfordres til

- for udvekslinger, hvor kanalen ikke er defineret i retsgrundlaget, at bruge Europol-kanalen baseret på SIENA-værktøjet som standardkanal, medmindre der er specifikke grunde til at anvende et andet instrument
- at udvikle nationale retningslinjer for valget af kanal
- når SIS II er taget i brug, og Sisnet er lukket, at bruge Europol-kanalen og SIENA-værktøjet til udveksling i forbindelse med politisamarbejde, hvor man i øjeblikket bruger Sisnet
- hvis det ikke allerede findes, at oprette et SPOC (en kvikskranke), som omfatter alle hovedkanaler, er døgnbemandet og samler alle retshåndhævende myndigheder, med adgang til nationale databaser
- at sikre, at oplysninger, der udveksles via politi- og toldsamarbejdscentre (PCCC'er), formidles til nationalt niveau (via SPOC) og til Europol, hvis det er hensigtsmæssigt
- at etablere samarbejde mellem SPOC'er og nationale koordinationscentre under Eurosur.

Rådet opfordres til

- at ændre retningslinjerne på EU-plan, så de afspejler de retningslinjer for valg af kanal, der foreslås ovenfor.

Kommissionen vil

- deltage i arbejdet for at vurdere mulighederne for at udvikle en platform til informationsudveksling.

3.3. Sikring af datakvalitet, -sikkerhed og -beskyttelse

Bestemmelserne om databeskyttelse i de eksisterende instrumenter skal overholdes. I henhold til Kommissionens forslag af 25. januar 2012 til direktiv om beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik

[31] Det Europæiske Agentur for den Operationelle Forvaltning af Store It-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed.

på at forebygge, efterforske, opdage eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger[32] skal databeskyttelsesreglerne i de eksisterende instrumenter revideres med henblik på at vurdere behovet for at tilpasse dem til dette direktiv.

Et **højt niveau af datasikkerhed** er nødvendigt for at beskytte integriteten af personoplysninger og sikre, at medlemsstaterne har tillid til udvekslingen af oplysninger. En kæde er ikke stærkere end det svageste led. Medlemsstater og EU-agenturer skal sikre, at data udveksles via meget sikre netværk. Ovennævnte direktivforslag indeholder bestemmelser om datasikkerhed[33], og på EU-plan er der fastlagt detaljerede sikkerhedsregler for beskyttelse af EU's klassificerede oplysninger[34].

Et **højt niveau af datakvalitet** er lige så vigtigt. "Arbejdsgangen", dvs. hvordan informationsudveksling gennemføres i praksis, er relevant i denne sammenhæng. Dette omfatter bl.a. **automatisering af specifikke opgaver**, når det er muligt og hensigtsmæssigt. Udformning af en anmodning om oplysninger fra en anden medlemsstat kræver f.eks., at data, der er registreret i et nationalt system, indtastes igen i det anvendte kommunikationsværktøj. Denne manuelle arbejdsgang kan medføre fejl og er tidskrævende. Sådanne opgaver kan automatiseres ved hjælp af **UMF II**[35], en anden IMS-foranstaltning. Dette EU-finansierede projekt, som ledes af Europol, har til formål at udvikle en standard for formatet af de meddelelser, der bruges til at anmode om oplysninger og til at sende svar. Derved kan dataoverførslen mellem forskellige systemer, f.eks. nationale sagsbehandlingssystemer og SIENA, automatiseres. Ud over potentielle omkostningsbesparelser eller i det mindste bedre ressourceudnyttelse opnås der dobbelte fordele ved at eliminere manuel genindtastning af data. Der frigives personale, som kan buges til valideringsopgaver. Ved at reducere omfanget af indtastningsfejl og lette udvekslingen af oplysninger i strukturerede formater forbedrer det desuden håndteringen og beskyttelsen af data.

Automatisering af opgaver betyder ikke, at hver eneste politibetjent i EU skal have adgang til alle politioplysninger i hele EU. Udveksling skal begrænses til det, der er nødvendigt og hensigtsmæssigt, og behovet skal forvaltes, så udveksling begrænses i overensstemmelse hermed. **Automatiske søgninger som en løsning på kapacitetsproblemer fungerer derfor som et system med hit/ikke-hit under EU's eksisterende instrumenter til informationsudveksling** (f.eks. SIS og dna og fingeraftryk, jf. Prümafgørelsen) eller er begrænset til snævert definerede datatyper (f.eks. oplysninger i køretøjsregistre, jf. Prümafgørelsen). Visse opgaver kan og bør ikke automatiseres, f.eks. validering af anmodninger og svar. Dette er især vigtigt i henhold til det svenske initiativ, som kræver, at anmodninger begrundes.

Endelig kan **interoperabilitet** mellem forskellige nationale systemer og administrative strukturer sikre fordele med hensyn til ensartede procedurer, kortere svartider, bedre datakvalitet og forenklet design og udvikling. Den europæiske interoperabilitetsramme[36] identificerer fire niveauer af interoperabilitet: teknisk, semantisk, organisatorisk og juridisk.

---

32 KOM(2012) 10.
33 Forslagets artikel 27-29.
34 Rådets afgørelse 2011/292/EU.
35 **U**niversal **M**essage **F**ormat.
36 KOM(2010) 744.

UMF II udvikler det semantiske niveau[37]. Tilpasning til fælles praksis (SPOC'er og valg af kanal) vil styrke det organisatoriske niveau. Oplysninger må dog kun udveksles og anvendes, når det er tilladt i henhold til lovgivningen.

Europol og medlemsstaterne opfordres til

- at fortsætte udviklingen af UMF II-standarden.

3.4. Forbedret uddannelse og bevidstgørelse

For at sikre, at retshåndhævelsespersonalet har den viden og de kompetencer, det skal bruge for at samarbejde effektivt, udarbejder Kommissionen en europæisk uddannelsesordning for retshåndhævelsespersonale. En kortlægning har påvist, at relevante EU-instrumenter til informationsudveksling er omhandlet i de retshåndhævende myndigheders grunduddannelse, men man har ikke vurderet kvaliteten af undervisningen. Specialiserede medarbejdere, f.eks. medarbejderne i SPOC'er, har brug for mere dybdegående uddannelse. Udveksling af sådanne medarbejdere vurderes[38] også at være gavnlig og bør tilskyndes.

Medlemsstaterne opfordres til

- at sikre, at retshåndhævelsespersonale modtager relevant uddannelse i grænseoverskridende informationsudveksling
- at tilrettelægge udveksling af SPOC-personale.

Kommissionen vil

- sikre, at den europæiske uddannelsesordning for retshåndhævelsespersonale omfatter uddannelse i grænseoverskridende informationsudveksling.

3.5. Finansiering

EU-finansieringen under særprogrammet "Forebyggelse og bekæmpelse af kriminalitet" (ISEC) er tildelt informationsudvekslingsprojekter, som f.eks. UMF II (830 000 EUR) og gennemførelse af Prüm (11,9 mio. EUR). Særprogrammet erstattes i 2014-20 af Fonden for Intern Sikkerhed, hvorunder EU-informationsudvekslingsprojekter også er støtteberettigede.

En del af Fonden for Intern Sikkerhed forvaltes af medlemsstaterne via såkaldt "delt forvaltning" i overensstemmelse med **flerårige programmer. Disse programmer bør inddrage relevante nationale prioriteter for informationsudveksling** i overensstemmelse med anbefalingerne i meddelelsen. Kommissionen vil parallelt hermed overveje, hvordan dele af Fonden for Intern Sikkerhed, som den forvalter direkte, kan støtte pilotprojekter, f.eks. ved at videreudvikle UMF II.

Hvad angår medlemsstaternes egne udgifter, kan andre anbefalede foranstaltninger (vedrørende SPOC'er og UMF II) bidrage til omkostningsbesparelser eller i det mindste bedre udnyttelse af ressourcer.

---

[37] UMF II tager andre projekter vedrørende semantik i betragtning, f.eks. fælles datamodeller, der udvikles under EU-programmet vedrørende interoperabilitetsløsninger for europæiske offentlige myndigheder.

[38] 10333/12.

Medlemsstaterne opfordres til

- at inddrage relevante prioriteter for informationsudveksling i nationale flerårige programmer under EU's Fond for Intern Sikkerhed for perioden 2014-20.

Kommissionen vil

- medtage politikker for informationsudveksling i ISF-programmeringsdialoger med medlemsstaterne

- opfordre til forslag til direkte finansiering (fra Kommissionen) af relevante pilotprojekter.

3.6. Statistik

De eksisterende statistikker (f.eks. SIS og SIENA) er ikke omfattende, selv om de er gode på nogle områder. Bedre statistikker vil forbedre kendskabet til anvendelsen af det svenske initiativ (for hvilket der kun findes tal indgivet ved hjælp af SIENA) og Prüm.

Indsamling af statistiske oplysninger kan dog være ressourcekrævende, navnlig hvis det ikke sker som led i den almindelige arbejdsgang. Ad hoc-indsamling bør undgås. Der foretrækkes en udviklingsbaseret tilgang, som tager udgangspunkt i processer, der allerede er indledt, f.eks. identifikation af Prümhits, der har været en hjælp i efterforskninger, som beskrevet i Prümrapporten. Øget brug af SIENA til anmodninger i henhold til det svenske initiativ som anbefalet ovenfor vil bevirke, at flere sådanne anmodninger vil blive afspejlet i SIENA-statistikker.

Medlemsstaterne opfordres til

- at forbedre statistikkerne om Prümforanstaltninger.

4. KONKLUSIONER

Forbedring af den grænseoverskridende informationsudveksling er ikke et mål i sig selv. Formålet er at tackle kriminalitet mere effektivt og reducere skadevirkningerne for ofrene og den europæiske økonomi.

Den grænseoverskridende informationsudveksling fungerer generelt godt og yder, som det fremgår af eksemplerne ovenfor, et værdifuldt bidrag i kampen mod alvorlig og grænseoverskridende kriminalitet i EU. Der er dog plads til forbedringer. Vedtaget lovgivning skal gennemføres fuldt ud af alle medlemsstater. I fremtiden bør medlemsstaterne alle bestræbe sig på mere systematisk at anvende Europol-kanalen og udvikle omfattende nationale kvikskranker (SPOC'er).

Kommissionen vil fra sin side fortsætte arbejdet med at kontrollere, hvordan instrumenterne gennemføres og anvendes, tilvejebringe EU-støtte og samle de forskellige aspekter for at sikre konsekvens. Kommissionen foreslår ikke et nyt instrument i dette tilfælde. Hvis den gør det i fremtiden, vil den følge de materielle principper i oversigten over informationsstyring fra 2010, nemlig sikring af grundlæggende rettigheder og sikring af nødvendighed, nærhed og præcis risikostyring.

Der kræves en målrettet indsats i Europol for at sikre, at relevante oplysninger deles, således at der skabes et dækkende billede af den grænseoverskridende kriminalitet i EU. Kommissionens kommende forslag til en Europol-reform vil imødekomme dette behov. Leveringen af oplysninger til Europol vil dog allerede blive styrket ved hjælp af denne meddelelses anbefalinger vedrørende mere systematisk anvendelse af Europol-kanalen og dens sikre kommunikationsværktøj SIENA.

For at følge op på denne meddelelse vil Kommissionen fortsat samarbejde med medlemsstaterne inden for rammerne af EU's informationsstyringsstrategi for intern sikkerhed, og den foreslår, at Rådet afholder en årlig debat i Den Stående Komité for den Indre Sikkerhed. Kommissionen opfordrer også Parlamentet til at drøfte disse anbefalinger, herunder i Det Særlige Udvalg om Organiseret Kriminalitet, Korruption og Hvidvaskning af Penge.