EUROPA-KOMMISSIONEN

Bruxelles, den 20.7.2010

KOM(2010)385 endelig

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed

1. INDLEDNING

Den Europæiske Union er nået langt, siden lederne af fem europæiske lande i 1985 i Schengen enedes om at ophæve kontrollen ved deres fælles grænser. Deres aftale førte i 1990 til Schengeaftalen, som indeholdt kimen til mange af nutidens politikker for informationsstyring. Ophævelsen af kontrollen ved de indre grænser har ført til udvikling af en række foranstaltninger ved de ydre grænser, navnlig vedrørende udstedelse af visa, koordinering af asyl- og indvandringspolitikker og styrkelse af politisamarbejdet, det retlige samarbejde og toldsamarbejdet i bekæmpelsen af grænseoverskridende kriminalitet. Hverken Schengenområdet eller det indre marked kunne i dag fungere uden grænseoverskridende informationsudveksling.

Terrorangrebene i USA i 2001 og bombeattentaterne i Madrid og London i henholdsvis 2004 og 2005 udløste en ny dynamik i udviklingen af EU's politikker for informationsstyring. I 2006 vedtog Rådet og Europa-Parlamentet datalagringsdirektivet, der skulle give de nationale myndigheder mulighed for at bekæmpe alvorlig kriminalitet ved at lagre telekommunikationsdata og lokaliseringsdata[1]. Efterfølgende gik Rådet videre med det svenske initiativ om forenkling af grænseoverskridende udveksling af oplysninger om strafferetlig efterforskning og efterretningsoperationer. I 2008 godkendte Rådet Prümafgørelsen om intensivering af udvekslingen af DNA-profiler, fingeraftryksoplysninger og oplysninger i køretøjsregistre i bekæmpelsen af terrorisme og andre former for kriminalitet. Grænseoverskridende samarbejde mellem finansielle efterretningsenheder, kontorer for inddrivelse af aktiver og platforme for it-kriminalitet, og medlemsstaternes brug af Europol og Eurojust er yderligere værktøjer i bekæmpelsen af alvorlig kriminalitet i Schengenområdet.

I efterdønningerne af terrorangrebene den 11. september 2001 iværksatte USA's regering sit program til sporing af finansiering af terrorisme for at forhindre lignende hændelser ved at overvåge mistænkelige finansielle transaktioner. Europa-Parlamentet har netop tilsluttet sig indgåelsen af aftalen mellem Den Europæiske Union og Amerikas Forenede Stater om overførsel af oplysninger om finansielle betalingsdata fra Den Europæiske Union til USA til brug for programmet til sporing af finansiering af terrorisme (TFTP-aftalen mellem EU og

[1] Der er ikke på nuværende tidspunkt en harmoniseret EU-definition af "alvorlig kriminalitet". I Rådets afgørelse om Europols adgang til at søge i VIS (Rådets afgørelse 2008/633/RIA), EUT L 218 af 13.8.2008, s. 129) defineres "alvorlige strafbare handlinger" med henvisning til den liste af strafbare handlinger der findes i den europæiske arrestordre (rammeafgørelse 2002/584/RIA, EFT L 190 af 18.7.2002, s. 1). Direktivet om lagring af data (direktiv 2002/58/EF, EUT L 105 af 13.4.2006, s. 54.) overlader det til medlemsstaterne af definere "alvorlig kriminalitet". Afgørelsen om oprettelse af Europol (Rådets afgørelse 2009/371/RIA, EUT L 121 af 15.5.2009, s. 37) indeholder en anden liste over overtrædelser, der defineres som "alvorlig kriminalitet", som i høj grad ligner listen i den europæiske arrestordre.

USA)[2]. Udvekslingen af passagerlisteoplysninger (Passenger Name Records, PNR) har også givet EU mulighed for bedre at bekæmpe terrorisme og andre former for alvorlig kriminalitet[3]. Efter at have indgået PNR-aftaler med USA, Australien og Canada er Kommissionen for nylig gået tilbage til tegnebrættet for at genoverveje sin tilgang til indførelse af et PNR-system i EU og udveksling af sådanne oplysninger med tredjelande.

Ovennævnte foranstaltninger har givet mulighed for fri bevægelighed i Schengenområdet, bidraget til forebyggelse og bekæmpelse af terrorangreb og andre former for alvorlig kriminalitet og fremmet udviklingen af en fælles visum- og asylpolitik.

Denne meddelelse giver for første gang et fuldstændigt overblik over instrumenter på EU-niveau, der allerede anvendes, er ved at blive gennemført eller overvejes, og som regulerer indsamling, lagring og grænseoverskridende udveksling af personoplysninger med henblik på retshåndhævelse og migrationsforvaltning. Borgerne har ret til at få oplyst, hvilke personoplysninger der behandles og udveksles om dem, af hvem og med hvilket formål. Dette dokument giver et åbent svar på disse spørgsmål. Det afdækker hovedformålet med disse instrumenter, deres struktur, den type personoplysninger, de dækker, listen over myndigheder med adgang til sådanne oplysninger og bestemmelser om databeskyttelse og lagring. Endvidere indeholder det et begrænset antal eksempler, der viser, hvordan instrumenterne fungerer i praksis (se bilag I). Endelig fastslås de hovedprincipper, der bør ligge til grund for udformning og evaluering af instrumenter til informationsstyring på området frihed, sikkerhed og retfærdighed.

Meddelelsen giver en oversigt over foranstaltninger på EU-niveau, der regulerer styringen af personoplysninger, og foreslår en række principper for udvikling og vurdering af sådanne foranstaltninger, og bidrager derved til en oplyst strategidialog med alle aktører. Samtidig er den en første reaktion på medlemsstaternes opfordringer til at udvikle en mere "sammenhængende" tilgang til udveksling af personoplysninger med henblik på retshåndhævelse som netop omhandlet i EU's informationsstyringsstrategi[4] og overvejelser om et eventuelt behov for at udvikle en europæisk model for informationsudveksling baseret på en evaluering af de nuværende foranstaltninger til informationsudveksling[5].

Formålsbegrænsning er et afgørende aspekt for de fleste instrumenter, der omtales i denne meddelelse. Et enkelt, overordnet og flerstrenget EU-informationssystem vil give den mest udbyggede informationsdeling. Indførelse af et sådant system vil imidlertid udgøre en alvorlig og ulovlig begrænsning af den enkeltes ret til privatliv og beskyttelse af personoplysninger og give store udfordringer, hvad angår udvikling og drift. I praksis har politikker på området frihed, sikkerhed og retfærdighed udviklet sig gradvist, og det har medført en række informationssystemer og instrumenter med varierende størrelse, anvendelsesområde og formål. Den opsplittede struktur for informationsstyring, der har udviklet sig i de seneste

---

2 Europa-Parlamentets beslutning P7_TA-PROV(2010)0279 af 8.7.2010.

3 I modsætning til alvorlig kriminalitet er "terrorhandlinger" klart defineret i Rådets afgørelse om bekæmpelse af terrorisme (Rådets rammeafgørelse 2002/475/RIA, EFT L 164 af 22.6.2002, s. 3). Ændret ved Rådets rammeafgørelse 2008/919/RIA, EUT L 330 af 9.12.2008, s. 21.

4 Rådets konklusioner om en informationsstyringsstrategi for EU's indre sikkerhed, Rådet (retlige og indre anliggender, 30.11.2009) (EU-informationsstyringsstrategi); Frihed, sikkerhed, privatlivets fred - europæiske indre anliggender i en åben verden; Rapport fra Den Uformelle Rådgivende Højniveaugruppe om Fremtiden for den Europæiske Politik vedrørende Indre Anliggender ("Fremtidsgruppen"), juni 2008.

5 Stockholmprogrammet - Et åbent og sikkert Europa i borgernes tjeneste og til deres beskyttelse, Rådets dokument 5731/10 af 3.3.2010, afsnit 4.2.2.

årtier, bidrager i højere grad til at beskytte borgernes ret til privatlivets fred end et centraliseret alternativ.

Denne meddelelse dækker ikke foranstaltninger, der involverer udveksling af andre oplysninger end personoplysninger til strategiske formål, som f.eks. generelle risikoanalyser eller trusselsvurderinger; den analyserer heller ikke i detaljer de omhandlede instrumenters bestemmelser om databeskyttelse, da Kommissionen i øjeblikket på basis af artikel 16 i traktaten om Den Europæiske Unions funktionsmåde har iværksat et særskilt initiativ om en ny, overordnet ramme for beskyttelse af personoplysninger i EU. Rådet behandler i øjeblikket udkastet til forhandlingsdirektiver for en aftale mellem EU og USA om beskyttelse af personoplysninger, når de overføres og behandles med henblik på at forebygge, undersøge, afsløre eller retsforfølge strafferetlige overtrædelser, herunder terrorisme, inden for rammerne af politisamarbejdet og det retlige samarbejde i straffesager. Da disse forhandlinger forventes at fastlægge den måde, hvorpå de to parter kan sikre et højt beskyttelsesniveau for grundlæggende rettigheder og frihedsrettigheder i forbindelse med overførsel eller behandling af personoplysninger snarere end selve indholdet af sådanne overførsler eller behandlinger, dækker denne meddelelse ikke dette initiativ[6].

2. EU-INSTRUMENTER TIL REGULERING AF INDSAMLING, LAGRING ELLER UDVEKSLING AF PERSONOPLYSNINGER MED HENBLIK PÅ RETSHÅNDHÆVELSE OG INDVANDRING

Dette afsnit giver en oversigt over Den Europæiske Unions instrumenter til regulering af indsamling, lagring eller grænseoverskridende udveksling af personoplysninger med henblik på retshåndhævelse og indvandring. Afsnit 2.1 fokuserer på foranstaltninger, der allerede anvendes, er ved at blive gennemført eller overvejes; afsnit 2.2 omhandler initiativer i henhold til handlingsprogrammet for Stockholmprogrammet[7]. Der gives oplysninger om følgende aspekter af hvert enkelt instrument:

– baggrund (om foranstaltningen er foreslået af medlemsstaterne eller af Kommissionen)[8]

– formålet/formålene med indsamling, lagring eller udveksling af oplysninger

– struktur (centraliseret informationssystem eller decentraliseret udveksling af oplysninger)

– type personoplysninger

– myndigheder med adgang til oplysningerne

– databeskyttelsesbestemmelser

---

6 KOM(2010) 252 af 26.5.2010.

7 KOM(2010) 171 af 20.4.2010 (Stockholmprogrammets handligsplan).

8 I Den Europæiske Unions tidligere tredje søjle om politisamarbejde og retligt samarbejde i straffesager havde medlemsstaterne og Kommissionen fælles initiativret. Med Amsterdamtraktaten blev områderne vedrørende kontrol ved de ydre grænser, visa, asyl og indvandring indarbejdet i Fællesskabets (første) søjle, hvor det udelukkende var Kommissionen, der havde initiativret. Lissabontraktaten har fjernet EU's søjlestruktur og fastslået Kommissionens initiativret. Inden for politisamarbejdet og det retlige samarbejde i straffesager (herunder administrativt samarbejde), kan en fjerdedel af medlemsstaterne imidlertid fortsat foreslå lovgivning.

– datalagringsregler

– gennemførelsesfase

– revisionsbestemmelser.

2.1. Instrumenter, der anvendes, er ved at blive gennemført eller overvejes

EU-instrumenter til fremme af Schengenområdets drift og toldunionen

Schengen-informationssystemet (SIS) opstod som et resultat af medlemsstaternes ønske om at oprette et område uden kontrol ved de indre grænser, samtidig med at det blev lettere at passere de ydre grænser[9]. Systemet har været i drift siden 1995 og har til formål at sikre den offentlige orden, herunder den nationale sikkerhed, i Schengenområdet og fremme borgernes bevægelighed ved at bruge oplysninger, der udveksles via dette system. SIS er et centraliseret informationssystem, der består af en national del i de deltagende stater og en teknisk støttefunktion i Frankrig. Medlemsstaterne kan foretage indberetninger for personer, der begæres anholdt med henblik på udlevering, tredjelandsstatsborgere, der nægtes indrejse, forsvundne personer, vidner eller andre indkaldte, personer og køretøjer, der er underkastet særlig overvågning på grund af den trussel, de udgør for den offentlige orden eller den nationale sikkerhed, bortkomne eller stjålne køretøjer, dokumenter og våben og mistænkelige pengesedler. Data registreret i SIS omfatter navne og kaldenavne, fysiske karakteristika, fødested og -dato, nationalitet og oplysninger om, hvorvidt den pågældende er bevæbnet og voldelig. Politi, grænsekontrol, toldmyndigheder og retlige myndigheder i straffesager har inden for rammerne af deres respektive retlige beføjelser adgang til ovennævnte. Indvandringsmyndigheder og konsulater har adgang til oplysninger om tredjelands-statsborgere, der er opført på lister over personer med forbud mod indrejse og indberetninger om bortkomne og stjålne dokumenter. Europol har adgang til visse kategorier af SIS-data, herunder indberetninger om personer, der begæres anholdt med henblik på udlevering, og om personer, der er underkastet særlig overvågning på grund af den trussel, de udgør for den offentlige orden eller den nationale sikkerhed. Eurojust har adgang til indberetninger om personer, der begæres anholdt med henblik på udlevering, og indberetninger om vidner eller andre indkaldte. Personoplysninger må udelukkende bruges med henblik på de specifikke indberetninger, som de blev videregivet til. Personoplysninger, der registreres i SIS med henblik på at spore personer, må kun opbevares, så længe de er nødvendige for udførelsen af de opgaver, de blev videregivet til, og højst tre år efter registreringen. Oplysninger om personer, der er underkastet særlig overvågning på grund af den trussel, de udgør for den offentlige orden eller den nationale sikkerhed, skal slettes efter et år. Medlemsstaterne skal vedtage nationale regler, der giver et databeskyttelsesniveau, der mindst svarer til det niveau, der følger af Europarådets konvention fra 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger Europarådets ministerkomités henstilling om politiets brug af personoplysninger[10]. Schengenaftalen indeholder ingen bestemmelser om revision, men de undertegnende parter kan foreslå ændringer hertil, hvorefter den ændrede tekst skal godkendes med enstemmighed og

---

9 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.

10 Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

ratificeres af de nationale parlamenter. SIS anvendes fuldt ud i 22 medlemsstater samt i Schweiz, Norge og Island. Det Forenede Kongerige og Irland deltager i de politiretlige aspekter af Schengenaftalen og SIS, bortset fra indberetninger om tredjelandsstatsborgere med indrejseforbud. Cypern har undertegnet Schengenkonventionen, men endnu ikke gennemført den. Liechtenstein forventes at gennemføre den i 2010; Bulgarien og Rumænien forventes at gennemføre den i 2011. Søgninger i SIS giver et "hit", når oplysningerne om den søgte person eller genstand matcher oplysninger i en eksisterende indberetning. Når de retshåndhævende myndigheder får et hit, kan de via deres netværk af SIRENE-kontorer anmode om yderligere oplysninger om genstanden for en indberetning[11].

I takt med at nye medlemsstater har tilsluttet sig Schengenområdet, er SIS-databasen vokset tilsvarende: mellem januar 2008 og 2010 steg det samlede antal SIS-indberetninger fra 22,9 til 31,6 millioner[12]. For at foregribe en sådan stigning i datamængder og ændrede brugerbehov besluttede medlemsstaterne i 2001 at udvikle **anden generation af Schengen-informationssystemet** (SIS II) og overlod denne opgave til Kommissionen[13]. SIS II er ved at blive udviklet og har til formål at sikre et højt sikkerhedsniveau på området frihed, sikkerhed og retfærdighed ved at styrke funktionerne i første generation af systemet og fremme borgernes bevægelighed ved at bruge oplysninger, der udveksles via dette system. Ud over de oprindelige datakategorier, der dækkes af førstegenerationssystemet, vil SIS II kunne behandle fingeraftryk, fotografier, kopier af den europæiske arrestordre, foranstaltninger til beskyttelse af de personers interesser, hvis identitet er blevet misbrugt, og forbindelser mellem forskellige indberetninger. F.eks. vil SIS II kunne forbinde indberetninger vedrørende en person, der efterlyses for bortførelse, den bortførte person og den bil, der er brugt til denne forbrydelse. Adgangsrettighederne og reglerne for datalagring er de samme som dem, der gælder for førstegenerationssystemet. Personoplysninger må udelukkende bruges med henblik på de specifikke indberetninger, som de blev videregivet til. Personoplysninger i SIS II skal behandles i overensstemmelse med de specifikke bestemmelser i den grundlæggende retsakt for systemet (forordning (EF) nr. 1987/2006 og Rådets afgørelse 2007/533/RIA), der afklarer principperne i direktiv 95/46/EF, og i overensstemmelse med forordning (EF) nr. 45/2001, Europarådets konvention 108 og henstilling om politiets brug af personoplysninger[14]. SIS II vil anvende s-TESTA, som er Kommissionens sikrede kommunikationsnet[15]. Når systemet bliver operationelt, vil det blive anvendt i alle medlemsstater, Schweiz, Liechtenstein, Norge og Island[16]. Kommissionen skal ved udgangen af hvert halvår forelægge Europa-Parlamentet

---

11 SIRENE står for anmodning om supplerende oplysninger ved det nationale grænseovergangssted (Supplementary Information Request at National Entry).

12 Rådets dokument 5441/08 af 30.1.2008; Rådets dokument 6162/10 af 5.2.2010.

13 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; afgørelse 2007/533/RIA, EUT L 205 af 7.8.2007, s. 63.

14 Forordning (EF) nr. 1987/2006, EUT L 381 af 28.12.2006, s. 4; afgørelse 2007/533/RIA, EUT L 205 af 7.8.2007, s. 63; direktiv 95/46/EF, EFT L 281 af 23.11.1995, s. 31; forordning (EF) nr. 45/2001, EFT L 8 af 12.1.2001, s. 1. Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

15 S-TESTA, som står for sikre transeuropæiske telematiktjenester mellem administrationer, er et kommunikationsnet finansieret af Kommissionen, som muliggør sikker og krypteret udveksling af data mellem nationale administrationer, EU-institutioner, agenturer og organer.

16 Det Forenede Kongerige og Irland deltager i SIS II, bortset fra indberetninger om tredjelandsstatsborgere med indrejseforbud.

og Rådet en statusrapport om udviklingen af SIS II og den potentielle overgang fra førstegenerationssystemet[17].

Udviklingen af **EURODAC** kan føres tilbage til ophævelsen af de indre grænser, som gjorde det nødvendigt at indføre klare regler for behandling af asylansøgninger. EURODAC er et centraliseret automatisk fingeraftryksidentifikationssystem, der indeholder fingeraftryksoplysninger for visse tredjelandsstatsborgere. Systemet har været i drift siden januar 2003 og har til formål at hjælpe med at fastslå, hvilken medlemsstat, der ifølge Dublin-forordningen er ansvarlig for at behandle en given asylansøgning[18]. Personer på over 14 år, som ansøger om asyl i en medlemsstat, vil automatisk få taget deres fingeraftryk, og det samme gælder tredjelandsstatsborgere, der pågribes i forbindelse med ulovlig passage af en ydre grænse. Ved at sammenligne disse personers fingeraftryk med EURODAC's registreringer, forsøger de nationale myndigheder at fastslå, hvor den pågældende person kan have indgivet en asylansøgning eller foretaget den første indrejse i Den Europæiske Union. Myndighederne kan også tjekke fingeraftryk for tredjelandsstatsborgere, der opholder sig ulovligt på deres område i EURODAC's registreringer. Medlemsstaterne skal præcisere, hvilke myndigheder der har adgang til denne database, typisk bl.a. asyl- og indvandringsmyndigheder, grænsevagter og politi. Medlemsstaterne registrerer de relevante data i den centrale database via deres nationale adgangspunkter. Personoplysninger i EURODAC kan kun bruges med henblik på at lette anvendelsen af Dublin-forordningen; al anden brug er strafbar. Asylansøgeres fingeraftryk lagres i 10 år; ulovlige indvandreres fingeraftryk i to år. Oplysninger om asylansøgere slettes, når de opnår statsborgerskab i en medlemsstat; ulovlige indvandreres fingeraftryk slettes, når de får opholdstilladelse eller statsborgerskab eller forlader EU. Hvad angår behandling af personoplysninger inden for rammerne af dette instrument, finder direktiv 95/46/EF anvendelse[19]. EURODAC fungerer via Kommissionens s-TESTA-netværk og anvendes i alle medlemsstater samt i Norge, Island og Schweiz. En aftale om Liechtensteins tilslutning er ved at blive indgået. Kommissionen skal forelægge Europa-Parlamentet og Rådet en årlig rapport om driften af EURODAC's centrale enhed.

I efterdønningerne af 11. september 2001 besluttede medlemsstaterne at fremskynde gennemførelsen af en fælles visumpolitik ved at indføre en udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold[20]. Ophævelsen af de indre grænser har også gjort det lettere at misbruge medlemsstaternes visumordninger. **Visuminformationssystemet** (VIS) tager sigte på at takle begge problemer: det har til formål at gennemføre en fælles visumpolitik ved at lette behandlingen af visumansøgninger og kontrollen ved de ydre grænser og samtidig bidrage til at forebygge trusler mod medlemsstaternes indre sikkerhed[21]. VIS er et centraliseret informationssystem, der består af en national del i de deltagende stater og en teknisk støttefunktion i Frankrig. Systemet vil bruge et biometrisk matchsystem for at sikre pålidelige fingeraftrykssammenligninger og kontrollere visumindehaveres identitet ved

---

17 Rådets forordning (EF) nr. 1104/2008, EUT L 299 af 8.11.2008, s. 1; Rådets afgørelse 2008/839/RIA, EUT L 299 af 8.11.2008, s. 43.

18 Rådets forordning (EF) nr. 343/2003, EUT L 50, 25.2.2003, s. 1 (Dublin-forordning), Rådets forordning (EF) 2725/2000, EFT L 316 af 15.12.2000, s. 1 (EURODAC-forordning). Disse instrumenter bygger på Dublin-konventionen fra 1990 (EFT C 254 af 19.8.1997, s. 1), der først forsøgte at fastslå, hvilken medlemsstat, der burde behandle asylansøgninger. Systemet vedrørende behandling af asylansøgninger er nu kendt som "Dublin-systemet".

19 Direktiv 95/46/EF, EFT L 281 af 23.11.1995, s. 31.

20 Ekstraordinært møde i Rådet (retlige og indre anliggender), 20.9.2001.

21 Rådets beslutning 2004/512/EF, EUT L 213 af 15.6.2004, s. 5; forordning (EF) nr. 767/2008, EUT L 218 af 13.8.2008, s. 60; Rådets afgørelse 2008/633/RIA, EUT L 218, 13.8.2008, s. 129. Se også erklæring om bekæmpelse af terrorisme, Det Europæiske Råd den 25.3.2004.

de ydre grænser. Det vil omfatte oplysninger om visumansøgninger, fotografier, fingeraftryk, relevante beslutninger fra visummyndigheder og forbindelser mellem tilknyttede ansøgninger. Visum-, asyl-, indvandrings- og grænsekontrolmyndigheder vil få adgang til denne database med henblik på at kontrollere visumindehaveres identitet og visummets ægthed; politiet og Europol kan søge i databasen for at forebygge og bekæmpe terrorisme og andre former for alvorlig kriminalitet[22]. Ansøgningsdossierer lagres i højst fem år. Personoplysninger i VIS skal behandles i overensstemmelse med de specifikke bestemmelser i den grundlæggende retsakt for dette system (forordning (EF) nr. 767/2008 og Rådets afgørelse 2008/633/RIA), der supplerer bestemmelserne i direktiv 95/46/EF, forordning (EF) nr. 45/2001, Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108, tillægsprotokol 181 og henstillingen om politiets brug af personoplysninger[23]. VIS vil finde anvendelse i alle medlemsstater (bortset fra Det Forenede Kongerige og Irland) samt i Schweiz, Norge og Island. Det skal drives på basis af Kommissionens sikrede kommunikationsnet s-TESTA. Kommissionen vil evaluere systemet tre år efter lanceringen og herefter hvert fjerde år.

På spansk initiativ vedtog Rådet i 2004 et direktiv om luftfartsselskabers fremsendelse til grænsekontrolmyndigheder af **forhåndsinformation om passagerer** (Advanced Passenger Information, API)[24]. Formålet med dette instrument er at forbedre grænsekontrollen og bekæmpe ulovlig indvandring. Luftfartsselskaber skal efter anmodning meddele grænsemyndighederne navn, fødselsdato, nationalitet, afrejsested og grænseovergangssted for passagerer, der rejser til EU fra tredjelande. Sådanne personoplysninger tages typisk fra den maskinlæsbare del på passagerers pas og fremsendes til myndighederne efter afslutning af check-in. Efter en flyankomst kan myndighederne og luftfartsselskaberne tilbageholde API-oplysninger i 24 timer. API-systemet er decentraliseret og sikrer udveksling af oplysninger mellem private operatører og offentlige myndigheder. Dette instrument giver ikke mulighed for udveksling af API-oplysninger mellem medlemsstater; imidlertid kan andre retshåndhævende myndigheder end grænsevagter anmode om adgang til disse oplysninger med henblik på retshåndhævelse. Personoplysninger kan kun bruges af offentlige myndigheder med henblik på grænsekontrol og bekæmpelse af ulovlig indvandring og skal behandles i overensstemmelse med direktiv 95/46/EF[25]. Dette instrument er trådt i kraft i hele EU, men anvendes kun af et lille antal medlemsstater. Kommissionen tager direktivet op til revision i 2011.

En vigtig del af Kommissionens 1992-program, der indførte det indre marked, vedrørte ophævelse af al kontrol og alle formaliteter for varebevægelser inden for Fællesskabet[26]. Ophævelsen af disse procedurer ved de indre grænser øgede risikoen for svig og krævede, at medlemsstaterne på den ene side indførte en mekanisme for gensidig administrativ bistand for at forebygge, efterforske og retsforfølge transaktioner, der udgør en overtrædelse af EU's told-

---

22 Rådets afgørelse 2008/633/RIA, EUT L 218 af 13.8.2008, s. 129.

23 Forordning (EF) nr. 767/2008, EUT L 218 af 13.8.2008, s. 60; Rådets afgørelse 2008/633/RIA, EUT L 218 af 13.8.2008, s. 129; direktiv 95/46/EF, EFT L 281 af 23.11.1995, s. 31; forordning (EF) nr. 45/2001, EFT L 8 af 12.1.2001, s. 1; Rådets rammeafgørelse 2008/977/RIA, EUT L 350 af 30.12.2008, s. 60; konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); tillægsprotokol til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, hvad angår tilsynsmyndigheder og overførsel af personoplysninger på tværs af grænserne (ETS nr. 181), Europarådet, 8.11.2001 (tillægsprotokol 181). Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

24 Rådets direktiv 2004/82/EF, EUT L 261 af 6.8.2004, s. 24.

25 Direktiv 95/46/EF, EFT L 281 af 23.11.1995, s. 31.

26 Rådets forordning (EF) nr. 2913/92, EFT L 302 af 19.10.1992.

og landbrugslovgivning, og på den anden side et toldsamarbejde, der muliggør afsløring og retsforfølgning af overtrædelser af de nationale toldbestemmelser, bl.a. ved at fremme den grænseoverskridende informationsudveksling. Uden at det berører EU's kompetence i toldunionen[27], tager **Napoli II-konventionen** om gensidig bistand og samarbejde mellem toldmyndighederne sigte på at give de nationale toldmyndigheder mulighed for at forebygge og afsløre overtrædelser af de nationale toldbestemmelser og hjælpe dem med at retsforfølge og straffe overtrædelser af EU's og medlemsstaternes toldbestemmelser[28]. Under dette instrument anmoder centrale koordineringsenheder skriftligt om bistand fra sådanne enheder i andre medlemsstater til strafferetlig efterforskning af overtrædelser af EU's eller nationale toldregler. Disse enheder kan kun behandle personoplysninger med henblik på Napoli II-konventionen. De kan fremsende sådanne oplysninger til nationale toldmyndigheder, efterforskningsmyndigheder og retlige myndigheder og til andre myndigheder, forudsat at den medlemsstat, der har videregivet oplysningerne, giver sit forudgående samtykke hertil. Oplysningerne må ikke opbevares længere end, hvad der er nødvendigt for udførelsen af de opgaver, hvortil de blev videregivet. Personoplysninger i den modtagende medlemsstat er omfattet af mindst samme beskyttelsesniveau som i den videregivende medlemsstat, og dens behandling skal opfylde bestemmelserne i direktiv 95/46/EF og Europarådets konvention 108[29]. Napoli II-konventionen er ratificeret af alle medlemsstater. De kan foreslå ændringer hertil, hvorefter den ændrede tekst skal vedtages af Ministerrådet og ratificeres af medlemsstaterne.

CIS-konventionen supplerer Napoli II-konventionen og er baseret på **Toldinformations-systemet** (CIS) til at forebygge, efterforske og retsforfølge alvorlige overtrædelser af national lovgivning ved gennem en hurtig spredning af oplysninger at effektivisere samarbejdet mellem medlemsstaternes toldmyndigheder[30]. CIS, der forvaltes af Kommissionen, er et centraliseret informationssystem tilgængeligt via terminaler i medlemsstaterne og i Kommissionen, Europol og Eurojust. Det omfatter personoplysninger med henvisning til varer, transportmidler, virksomheder, personer, varer og kontanter, der er tilbageholdt, beslaglagt eller konfiskeret. Personoplysningerne er navne og kaldenavne, fødselsdato og -sted, nationalitet, køn, fysiske karakteristika, identitetspapirer, adresse, tidligere tilfælde af vold, årsager til registrering af oplysninger i CIS, påtænkt aktion og registrering af transportmidler. Hvis der tilbageholdes, beslaglægges eller konfiskeres varer og kontanter, registreres kun personoplysninger og en adresse i CIS. Sådanne oplysninger må udelukkende bruges med henblik på observation, optagelse af rapport eller gennemførelse af særlige inspektioner, målrettet kontrol eller strategiske eller operationelle analyser vedrørende personer, der mistænkes for at have overtrådt de nationale toldbestemmelser. Nationale told-, skatte-, landbrugs-, sundheds- og politimyndigheder, Europol og Eurojust har adgang til

---

27 Rådets forordning (EF) nr. 515/97 af 13.3.1997 om gensidig bistand mellem medlemsstaternes administrative myndigheder og om samarbejde mellem disse og Kommissionen med henblik på at sikre den rette anvendelse af told- og landbrugsbestemmelserne, EFT L 82 af 22.3.1997, s. 1, ændret ved forordning (EF) nr. 766/2008, EUT L 218 af 13.8.2008, s. 48.

28 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 (Napoli II-konventionen).

29 Direktiv 95/46/EF, EFT L 281 af 23.11.1995, s. 31; konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108).

30 Konvention udarbejdet på grundlag af artikel K.3 i traktaten om Den Europæiske Union, om brug af informationsteknologi på toldområdet, EFT C 316 af 27.11.1995, s. 34, ændret ved Rådets afgørelse 2009/917/RIA, EUT L 323 af 10.12.2009, s. 20.

CIS-oplysninger[31]. Behandlingen af personoplysninger skal være i overensstemmelse med de specifikke regler i CIS-konventionen og bestemmelserne i direktiv 95/46/EF, forordning (EF) nr. 45/2001, Europarådets konvention 108 og henstillingen om politiets brug af personoplysninger[32]. Der kan kun kopieres personoplysninger fra CIS til andre databehandlingssystemer med henblik på risikostyring eller operationelle analyser, som kun analytikere udpeget af medlemsstaterne har adgang til. Personoplysninger kopieret fra CIS må kun opbevares så længe, det er nødvendigt for at opfylde det formål, hvortil de blev kopieret, og højst 10 år. CIS opretter også et **elektronisk sagsregister på toldområdet** (FIDE) for at bistå med at forebygge, efterforske og retsforfølge alvorlige overtrædelser af nationale love[33]. FIDE giver de nationale myndigheder, der har ansvaret for at foretage toldefterforskninger, mulighed for, når de åbner en efterforskningsfil, at identificere andre myndigheder, der måtte have efterforsket en givet person eller virksomhed. Disse myndigheder kan registrere oplysninger i FIDE fra deres efterforskningsfiler, herunder oplysninger om personer, der efterforskes, og firmanavn, momsnummer og adresse for den virksomhed, der efterforskes. Oplysninger fra efterforskningsfiler, hvor der ikke er afsløret toldsvig, kan opbevares i højst tre år; oplysninger fra filer, hvor der er afsløret toldsvig, kan opbevares i højst seks år; og oplysninger fra filer, hvor der foreligger en straffedom eller sanktion, kan opbevares i højst ti år. CIS og FIDE er baseret på Common Communication Network, Common System Interface eller sikker webadgang stillet til rådighed af Kommissionen. CIS er i kraft i alle medlemsstater. Kommissionen skal hvert år i samarbejde med medlemsstaterne forelægge Europa-Parlamentet og Rådet en rapport om driften af CIS.

EU-instrumenter, der tager sigte på at forebygge og bekæmpe terrorisme og andre former for alvorlig grænseoverskridende kriminalitet

Terrorattentaterne i marts 2004 i Madrid gav anledning til flere nye initiativer på EU-niveau. Efter anmodning fra Det Europæiske Råd fremlagde Kommissionen i 2005 et forslag til et instrument til regulering af udveksling af oplysninger efter tilgængelighedsprincippet[34]. I stedet for at godkende dette forslag vedtog Rådet i 2006 det **svenske initiativ**, som strømliner udvekslingen af eksisterende oplysninger eller strafferetlige efterretninger, som kunne være nødvendige i strafferetlig efterforskning og efterretningsoperationer[35]. Dette instrument er baseret på princippet om "lige adgang", ifølge hvilket betingelserne for grænseoverskridende udveksling af oplysninger ikke bør være mere restriktive end betingelserne for indenlandsk udveksling. Det svenske initiativ fungerer på decentral vis og giver politi, toldvæsen og andre myndigheder mulighed for at efterforske strafbare handlinger (med undtagelse af

---

31 Fra maj 2011 vil Europol og Eurojust få læseadgang til CIS, jf. Rådets afgørelse 2009/917/RIA, EUT L 323 af 10.12.2009, s. 20.

32 Konvention udarbejdet på grundlag af artikel K.3 i traktaten om Den Europæiske Union, om brug af informationsteknologi på toldområdet, EFT C 316 af 27.11.1995, s. 34, ændret ved Rådets afgørelse 2009/917/RIA, EUT L 323 af 10.12.2009, s. 20; direktiv 95/46/EF, EFT L 281 af 23.11.1995, s. 31; forordning (EF) nr. 45/2001, EFT L 8 af 12.1.2001, s. 1; konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

33 FIDE, som står for *Fichier d'Identification des Dossiers d'Enquêtes douanières*, er baseret på Rådets forordning (EF) nr. 766/2008 og protokollen udarbejdet i overensstemmelse med artikel 34 i traktaten om Den Europæiske Union, der, hvad angår oprettelsen af et elektronisk sagsregister på toldområdet, ændrer konventionen om brug af informationsteknologi på toldområdet, EUT C 139 af 13.6.2003, s. 1

34 KOM(2005) 490 af 12.10.2005; formandskabets konklusioner – Haagprogrammet, 4.-5.11.2004. Se også erklæring om bekæmpelse af terrorisme, Det Europæiske Råd den 25.3.2004.

35 Rådets rammeafgørelse 2006/960/RIA, EUT L 386, 29.12.2006, s. 89.

efterretningstjenester, som typisk behandler efterretninger i relation til national eller statslig sikkerhed) og udveksle oplysninger og kriminalefterretninger med deres modparter i EU. Medlemsstaterne skal udpege nationale kontaktpunkter, der skal håndtere hastende anmodninger om oplysninger. Denne foranstaltning fastsætter klare tidsfrister for udveksling af oplysninger og pålægger medlemsstaterne at udfylde en formular, når de anmoder om oplysninger. Medlemsstaterne skal besvare anmodninger om oplysninger og efterretninger inden for en frist på 8 timer i hastetilfælde, inden for en uge i ikke-hastende tilfælde og inden for to uger i alle andre tilfælde. Brug af oplysninger og efterretninger, der er opnået ved hjælp af dette instrument, er underkastet nationale databeskyttelseslove, hvor medlemsstaterne ikke har ret til at behandle oplysninger baseret på nationale kilder anderledes end oplysninger fra andre medlemsstater. Den videregivende medlemsstat kan imidlertid fastsætte betingelser for anvendelse af oplysninger eller efterretninger i andre medlemsstater. Personoplysninger skal behandles i overensstemmelse med national databeskyttelseslovgivning og Europarådets konvention 108, tillægsprotokol 181 og henstillingen om politiets brug af person-oplysninger[36]. 12 af de 31 signatarlande (EU-medlemsstaterne, Norge, Island, Schweiz og Liechtenstein) har vedtaget national lovgivning for at gennemføre initiativet; fem stater udfylder regelmæssigt formularen, når de anmoder om oplysninger, men kun to stater bruger den regelmæssigt til udveksling af oplysninger[37]. Kommissionen skal forelægge sin evalueringsrapport for Rådet inden udgangen af 2010.

Prümafgørelsen bygger på en aftale indgået af Tyskland, Frankrig, Spanien, Benelux og Østrig i 2005 om intensivering af samarbejdet om bekæmpelse af terrorisme, grænseoverskridende kriminalitet og ulovlig migration. Som svar på flere medlemsstaters interesse i at tiltræde denne aftale foreslog Tyskland under sit rådsformandskab i 2007 at omdanne den til et EU-instrument. Prümafgørelsen fra 2008, som skal være gennemført i august 2011, fastlægger reglerne for grænseoverskridende udveksling af DNA-profiler, fingeraftryk, oplysninger i køretøjsregistre og oplysninger om personer, der mistænkes for at planlægge terrorangreb[38]. Den har til formål at styrke forebyggelsen af strafbare handlinger, navnlig terrorisme og grænseoverskridende kriminalitet, og opretholde den offentlige orden i forbindelse med store begivenheder. Systemet er decentralt og vil fungere via nationale kontaktpunkter, der sammenkobler de deltagende staters databaser med DNA, fingeraftryk og køretøjsregistreringer. Ved hjælp af Kommissionens s-TESTA-netværk vil kontaktpunkterne behandle ind- og udgående anmodninger om grænseoverskridende sammenligninger af DNA-profiler, fingeraftryk og oplysninger i køretøjsregistre. Beføjelser til at fremsende sådanne oplysninger til slutbrugere er reguleret af national lov. Fra august 2011 vil data-sammenligningen ske automatisk. Medlemsstaterne skal imidlertid gennemgå en streng evalueringsproces (bl.a. en vurdering af, om de opfylder kravene til databeskyttelse og de tekniske krav) for at blive godkendt til automatisk udveksling af oplysninger. Der kan ikke udveksles personoplysninger i henhold til dette instrument, før medlemsstaterne har garanteret et databeskyttelsesniveau, der mindst svarer til det, der er fastsat i Europarådets konvention

---

[36] Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); tillægsprotokol til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, hvad angår tilsynsmyndigheder og overførsel af personoplysninger på tværs af grænserne (ETS nr. 181), Europarådet, 8.11.2001 (tillægsprotokol 181). Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

[37] Disse oplysninger er baseret på svar på et spørgeskema, hvis resultater det spanske formandskab fremlagde på et møde i ad hoc-arbejdsgruppen om informationsudveksling den 22.6.2010.

[38] Rådets afgørelse 2008/615/RIA, EUT L 210 af 6.8.2008, s. 1; Rådets afgørelse 2008/616/RIA, EUT L 210 af 6.8.2008, s. 12.

108, tillægsprotokol 181 og henstillingen om politiets brug af personoplysninger[39]. Rådet afgør med enstemmighed, om denne betingelse er opfyldt. Personoplysninger kan udelukkende anvendes til det formål, som de er videregivet til, medmindre den anmodede medlemsstat giver samtykke til anden brug. Borgerne kan også henvende sig til deres nationale databeskyttelsesansvarlige, der udpeges i medfør af direktiv 95/46/EF, for at håndhæve deres rettigheder vedrørende behandling af personoplysninger inden for rammerne af dette instrument. Sammenligning af DNA-profiler og fingeraftryk fungerer som et system med "hit/ikke-hit" (anonymt), og myndighederne kan kun anmode om personoplysninger om en registreret, hvis deres oprindelige søgning gav et hit. Sådanne anmodninger om yderligere oplysninger kanaliseres typisk via det svenske initiativ. Prümafgørelsen er gennemført i EU-27, og Norge og Island er ved at tilslutte sig[40]. Kommissionen skal forelægge sin evalueringsrapport for Rådet i 2012.

Som reaktion på bombeattentaterne i London i 2005 foreslog Storbritannien, Irland, Sverige og Frankrig at vedtage et EU-instrument om harmonisering af de nationale regler for datalagring. **Direktivet om lagring af data** fra 2006 forpligter telefon- og internetudbydere til med henblik på efterforskning, afsløring og retsforfølgning af alvorlig kriminalitet at lagre oplysninger om trafik og lokalisering samt oplysninger om abonnenter (herunder deres telefonnummer, IP-adresse og brugeridentitet)[41]. Direktivet om lagring af data regulerer hverken adgang til eller brugen af de oplysninger, de nationale myndigheder lagrer. Dets anvendelsesområde udelukker udtrykkeligt indholdet af elektronisk kommunikation; med andre ord er aflytning ikke mulig i henhold til dette instrument. Denne foranstaltning overlader det til medlemsstaterne at definere "alvorlig kriminalitet". Medlemsstaterne fastsætter også, hvilke nationale myndigheder der har adgang til sådanne oplysninger fra sag til sag samt procedurerne og betingelserne for at give adgang til oplysningerne. Perioderne for lagring af data svinger fra 6 til 24 måneder. Direktiv 95/46/EF og direktiv 2002/58/EF regulerer beskyttelse af personoplysninger under dette instrument[42]. Seks medlemsstater har endnu ikke fuldt ud gennemført denne foranstaltning, og forfatningsdomstolene i Tyskland og Rumænien har erklæret, at deres nationale gennemførelseslovgivning ikke er i overensstemmelse med forfatningen. Den tyske forfatningsdomstol fandt, at reglerne for adgang til og brug af oplysningerne som fastsat i national lov var i modstrid med forfatningen[43]. Den rumænske forfatningsdomstol fandt, at datalagring *per se* udgjorde en krænkelse af artikel 8 i konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (den europæiske menneskerettighedskonvention) og derfor var i modstrid med forfatningen[44]. Kommissionen er i øjeblikket ved at evaluere dette instrument og skal forelægge sin evalueringsrapport for Europa-Parlamentet og Rådet i slutningen af 2010.

---

39 Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); tillægsprotokol til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, hvad angår tilsynsmyndigheder og overførsel af personoplysninger på tværs af grænserne (ETS nr. 181), Europarådet, 8.11.2001 (Tillægsprotokol 181). Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

40 Indtil nu har 10 medlemsstater fået tilladelse til at begynde automatisk udveksling af DNA-profiler, fem har tilladelse til fingeraftryk og syv til oplysninger i køretøjsregistre. Tyskland, Østrig, Spanien og Nederlandene har givet Kommissionen delvise statistikker om deres brug af dette instrument.

41 Direktiv 2006/24/EF, EUT L 105 af 13.4.2006, s. 54.

42 Direktiv 95/46/EF, EFT L 281 af 23.11.1995, s. 31; direktiv 2002/58/EF, EFT L 201 af 31.7.2002, s. 37 (e-databeskyttelsesdirektivet).

43 Dom fra den tyske forfatningsdomstol, Bundesverfassunggericht 1 BvR 256/08, 11.3.2008.

44 Afgørelse nr. 1258 fra den rumænske forfatningsdomstol, 8.10.2009.

Den igangværende indførelse af et **europæisk informationssystem vedrørende strafferegistre** (ECRIS) kan føres tilbage til et belgisk initiativ fra 2004, der tog sigte på at udelukke personer, der er dømt for sædelighedskriminalitet, i at arbejde med børn i andre medlemsstater. Medlemsstaterne har hidtil baseret sig på Europarådets konvention om gensidig retshjælp i straffesager for at udveksle oplysninger om egne statsborgeres domfældelser, men det system har vist sig at være ineffektivt[45]. Rådet tog et første skridt mod en reform ved at vedtage Rådets afgørelse 2005/876/RIA, ifølge hvilken hver medlemsstat skal udpege en central myndighed, der regelmæssigt skal videresende oplysninger om straffedomme for statsborgere i andre medlemsstater til den medlemsstat, hvor de pågældende er statsborgere[46]. Dette instrument gav også for første gang medlemsstaterne mulighed for, med forbehold af national lovgivning, at få fremsendt tidligere straffedomme vedrørende deres egne statsborgere afsagt i andre medlemsstater. De kunne anmode om disse oplysninger ved at udfylde en standardformular i stedet for at anvende procedurerne for gensidig retshjælp. I 2006 og 2007 fremlagde Kommissionen en omfattende lovgivningspakke bestående af tre instrumenter, nemlig Rådets rammeafgørelse 2008/675/RIA, der forpligter medlemsstaterne til at tage hensyn til straffedomme afsagt i andre medlemsstater i Den Europæiske Union i forbindelse med en ny straffesag, Rådets rammeafgørelse 2009/315/RIA om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne og Rådets rammeafgørelse 2009/316/RIA om indførelse af ECRIS som et teknisk middel til at udveksle oplysninger fra strafferegistre[47]. Rådets rammeafgørelse 2009/315/RIA og 2009/316/RIA, der forventes gennemført i 2012, tager sigte på at definere, hvordan en domsstat skal formidle oplysninger om en ny dom til den dømte persons medlemsstat og fastsætter opbevaringsforpligtelser og rammer for et edb-baseret system til udveksling af oplysninger.ECRIS bliver et decentraliseret informationssystem, der sammenkobler medlemsstaternes databaser med strafferegistre via Kommissionens s-TESTA-netværk. De centrale myndigheder vil udveksle oplysninger om borgernes domfældelser og strafferegistre. Oplysningerne vil være krypterede og strukturerede i henhold til et forud defineret format og omfatte følgende: personlige oplysninger; dom, straf og selve overtrædelsen samt yderligere oplysninger (herunder eventuelt fingeraftryk). Fra april 2012 skal uddrag fra strafferegistre fremlægges i igangværende straffesager og fremsendes til de kompetente retlige og administrative myndigheder, f.eks. de instanser, der er bemyndiget til at vurdere personer, som ønsker at besætte et følsomt embede eller besidde våben. Personoplysninger, der formidles med henblik på straffesager, må kun bruges til det formål; brug til andet formål kræver samtykke fra den formidlende medlemsstat. Behandlingen af personoplysninger skal ske i overensstemmelse med bestemmelserne i Rådets rammeafgørelse 2009/315/RIA, der omfatter reglerne i Rådets afgørelse 2005/876/RIA, samt Rådets rammeafgørelse 2008/977/RIA og Europarådets konvention 108[48]. Hvad angår EU-institutionernes behandling af personoplysninger inden for rammerne af ECRIS, finder forordning (EF) nr. 45/2001 anvendelse for at sikre datasikkerhed[49]. Denne lovgivningspakke

---

45 Den europæiske konvention om gensidig retshjælp i straffesager (ETS nr. 30), Europarådet, 20.4.1959. Se også KOM(2005) 10 af 25.1.2005.

46 Rådets afgørelse 2005/876/RIA, EUT L 322 af 9.12.2005, s. 33.

47 Rådets rammeafgørelse 2008/675/RIA, EUT L 220 af 15.8.2008, s. 32; Rådets rammeafgørelse 2009/315/RIA, EUT L 93 af 7.4.2009, s. 23; Rådets afgørelse 2009/316/RIA, EUT L 93 af 7.4.2009, s. 33. Se også KOM(2005) 10 af 25.1.2005.

48 Rådets rammeafgørelse 2009/315/RIA, EUT L 93 af 7.4.2009, s. 23; Rådets afgørelse 2005/876/RIA, EUT L 322 af 9.12.2005, s. 33; Rådets rammeafgørelse 2008/977/RIA, EUT L 350 af 30.12.2008, s. 60; konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108).

49 Forordning (EF) nr. 45/2001, EFT L 8 af 12.1.2001, s. 1.

indeholder ikke regler om lagring af oplysninger, da lagring af oplysninger om straffedomme er reguleret af national lov. Femten medlemsstater deltager i øjeblikket i et pilotprojekt, og ni har indledt elektronisk udveksling af oplysninger fra strafferegistre. Kommissionen skal forelægge Europa-Parlamentet og Rådet to evalueringsrapporter om, hvordan denne lovgivningspakke virker: rammeafgørelse 2008/675/RIA skal revurderes i 2011, og rammeafgørelse 2009/315/RIA skal revurderes i 2015. Fra 2016 skal Kommissionen også udarbejde regelmæssige rapporter om ECRIS' drift.

På finsk initiativ vedtog Rådet i 2000 et instrument om udveksling af oplysninger mellem medlemsstaternes **finansielle efterretningsenheder** (Financial Intelligence Units, FIU) for at bekæmpe hvidvaskning af penge og terrorfinansiering[50]. FIU'er er typisk etableret inden for rammerne af retshåndhævende myndigheder, retlige myndigheder eller administrative organer, der rapporterer til finansielle myndigheder. De skal udveksle de nødvendige finansielle eller retslige oplysninger, herunder oplysninger om finansielle transaktioner, med deres EU-modparter, bortset fra de tilfælde hvor sådanne afsløringer ikke ville stå i et rimeligt forhold til de fysiske eller juridiske personers interesser. Oplysninger, der formidles med henblik på analyse eller undersøgelse af hvidvaskning eller terrorfinansiering, kan også bruges til strafferetlig efterforskning eller retsforfølgning, medmindre den formidlende medlemsstat forbyder en sådan brug. Behandlingen af personoplysninger skal være i overensstemmelse med bestemmelserne i Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108 og henstillingen om politiets brug af personoplysninger[51]. I 2002 oprettede flere medlemsstater FIU.net, en decentraliseret netværksapplikation, som behandler oplysninger, der udveksles mellem FIU'er og fungerer via Kommissionens s-TESTA-netværk[52]. Dette initiativ har tyve FIU'er som medlemmer. Der er drøftelser i gang om at anvende Europols sikre SIENA-applikation til drift af FIU.net[53]. Efter at have vurderet medlemsstaternes anvendelse af dette instrument, gav Rådet i det tredje direktiv om bekæmpelse af hvidvaskning FIU'erne beføjelser til at modtage, analysere og viderebringe efterretninger om mistænkelige transaktioner i relation til hvidvaskning og terrorfinansiering[54]. Som led i handlingsplanen for finansielle tjenesteydelser har Kommissionen siden 2009 revurderet gennemførelsen af det tredje direktiv om bekæmpelse af hvidvaskning af penge[55].

Efter et initiativ fra Østrig, Belgien og Finland vedtog Rådet i 2007 et instrument, der tager sigte på at fremme samarbejdet mellem **kontorer for inddrivelse af aktiver** (Asset Recovery Offices, ARO) i bestræbelserne på at spore og identificere udbyttet fra strafbart forhold[56]. I lighed med FIU'er samarbejder ARO'er på decentraliseret basis, dog uden bistand fra en onlineplatform. De skal bruge det svenske initiativ til at udveksle oplysninger, specificere detaljer om det omhandlede formuegode, som f.eks. bankkonti, fast ejendom og køretøjer, samt oplysninger om eftersøgte fysiske og juridiske personer, herunder deres navn, adresse,

---

50 Rådets afgørelse 2000/642/RIA, EFT L 271 af 24.10.2000, s. 4.

51 Rådets rammeafgørelse 2008/977/RIA, EUT L 350 af 30.12.2008, s. 60; konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

52 http://www.fiu.net/

53 SIENA står for Secure Information Exchange Network Application.

54 Direktiv 2005/60/EF, EUT L 309 af 25.11.2005, s. 15 (tredje direktiv om bekæmpelse af hvidvaskning af penge).

55 Se f.eks. Evaluation of the economic impacts of the Financial Services Action Plan – Final report (for for Europa-Kommissionen, GD MARKT), CRA International, 3.2009.

56 Rådets afgørelse 2007/845/RIA, EUT L 332 af 18.12.2007, s. 103.

fødselsdato og aktionær- og selskabsoplysninger. Brug af oplysninger, der udveksles inden for rammerne af dette instrument, er underkastet nationale databeskyttelseslove, hvor medlemsstaterne ikke har ret til at behandle oplysninger baseret på nationale kilder anderledes end oplysninger fra andre medlemsstater. Behandlingen af personoplysninger skal være i overensstemmelse med Europarådets konvention 108, tillægsprotokol 181 og henstilling om politiets brug af personoplysninger[57]. Indtil videre har over tyve medlemsstater oprettet ARO'er. Da der udveksles følsomme oplysninger, foregår der drøftelser om at anvende Europols SIENA-applikation for oplysninger, der udveksles mellem ARO'er. I et pilotprojekt lanceret i maj 2010 begyndte tolv kontorer for inddrivelse af aktiver at bruge SIENA til udveksling af oplysninger af interesse for sporing af aktiver. Kommissionen skal forelægge en evalueringsrapport for Rådet i 2010.

I 2008 opfordrede det franske formandskab medlemsstaterne til at etablere **nationale platforme for indberetning af it-kriminalitet** og Europol til at oprette en europæisk platform for indberetning af it-kriminalitet med henblik på at indsamle, analysere og udveksle oplysninger om lovovertrædelser begået på internettet[58]. Borgerne kan rapportere til deres nationale platforme om tilfælde med ulovligt indhold eller ulovlig adfærd, der konstateres på internettet. Den europæiske it-kriminalitetsplatform (European Cybercrime Platform, ECCP), der forvaltes af Europol, skal fungere som et informationscenter og analysere og udveksle oplysninger vedrørende it-kriminalitet, der falder ind under Europols mandat[59]. Indtil videre har næsten alle medlemsstater oprettet nationale platforme til indberetning af it-kriminalitet. Europol arbejder med den tekniske gennemførelse af den europæiske it-kriminalitetsplatform og forventes snart at anvende sin SIENA-applikation til at fremme udveksling af oplysninger med nationale platforme. I det omfang en sådan udveksling af oplysninger berører Europols behandling af personoplysninger, finder de specifikke bestemmelser om databeskyttelse i afgørelsen om oprettelse af Europol (Rådets afgørelse 2009/371/RIA) samt forordning (EF) 45/2001, Europarådets konvention 108 med tillægsprotokol 181 og henstillingen om politiets brug af personoplysninger anvendelse[60]. Bestemmelserne i Rådets rammeafgørelse 2008/977/RIA gælder for udveksling af personoplysninger mellem medlemsstaterne og Europol[61]. Da der ikke findes et retligt instrument, er der ingen formel revisionsmekanisme

---

57 Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); tillægsprotokol til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, hvad angår tilsynsmyndigheder og overførsel af personoplysninger på tværs af grænserne (ETS nr. 181), Europarådet, 8.11.2001 (tillægsprotokol 181). Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

58 Rådets konklusioner om etablering af nationale platforme og en europæisk platform for indberetning af strafbare handlinger på internettet, Rådet (retlige og indre anliggender), 24.10.2008; Rådets konklusioner om en handlingplan til gennemførelse af den samordnede strategi for bekæmpelse af kriminalitet, Rådet (almindelige anliggender), 26.4.2010. Europol har omdøbt sit projekt til "European Cybercrime Platform" (ECCP).

59 Europols formål er at forebygge og bekæmpe organiseret kriminalitet, terrorisme og andre former for alvorlig kriminalitet, der påvirker to eller flere medlemsstater. Se Rådets afgørelse 2009/371/RIA, EUT L 121 af 15.5.2009, s. 37.

60 Rådets afgørelse 2009/371/RIA, EUT L 121 af 15.5.2009, s. 37; forordning (EF) nr. 45/2001, EFT L 8 af 12.1.2001, s. 1; konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); tillægsprotokol til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, hvad angår tilsynsmyndigheder og overførsel af personoplysninger på tværs af grænserne (ETS nr. 181), Europarådet, 8.11.2001 (tillægsprotokol 181). Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

61 Rådets rammeafgørelse 2008/977/RIA, EUT L 350 af 30.12.2008, s. 60.

for it-kriminalitetsplatforme. Europol dækker imidlertid allerede dette vigtige område, og vil i fremtiden rapportere om den europæiske it-kriminalitetsplatforms aktiviteter i sin årsberetning, der forelægges Rådet til godkendelse og Europa-Parlamentet til orientering.

EU-agenturer og organer, der har beføjelser til at bistå medlemsstaterne med at forebygge og bekæmpe alvorlig grænseoverskridende kriminalitet

Den Europæiske Politienhed (Europol), der blev oprettet i 1995, startede sin drift i 1999 og blev et EU-agentur i januar 2010[62]. Europol skal støtte medlemsstaterne i deres bestræbelser på at forebygge og bekæmpe organiseret kriminalitet, terrorisme og andre former for alvorlig kriminalitet, der påvirker to eller flere medlemsstater. Europols hovedopgaver er at indsamle, lagre, behandle, analysere og udveksle oplysninger og efterretninger, bistå ved efterforskninger, stille efterretninger til rådighed og yde analytisk støtte til medlemsstaterne. Det vigtigste forbindelsesled mellem Europol og medlemsstaterne er Europols nationale enheder, som udstationerer forbindelsesofficerer ved Europol. Lederne af Europols nationale enheder mødes regelmæssigt for at bistå Europol med operative anliggender, og agenturets drift ledes af bestyrelsen og direktøren. Europols informationsbehandlingssystemer omfatter Europols informationssystem (EIS), analyseregistre (AWF) og SIENA-applikationen. Informationssystemet indeholder personoplysninger, herunder biometriske identifikatorer, afsagte domme og forbindelser til organiseret kriminalitet for personer, der mistænkes for kriminalitet inden for rammerne af Europols beføjelser. Adgangen er begrænset til Europols nationale enheder, forbindelsesofficerer, godkendt Europol-personale og direktøren. Analyseregistrene, der oprettes med det formål at understøtte strafferetlige efterforskninger, omfatter oplysninger om enkeltpersoner og andre oplysninger, som Europols nationale enheder kan beslutte at tilføje. Adgangen er begrænset til forbindelsesofficerer, men kun analytikere fra Europol kan indlæse oplysninger i registrene. Et indekssystem giver de nationale enheder og forbindelsesofficerer mulighed for at kontrollere, om et analyseregister indeholder oplysninger af interesse for deres medlemsstat. Europols SIENA-applikation bruges i stigende grad af medlemsstaterne til at udveksle følsomme oplysninger med henblik på retshåndhævelse. Europol kan behandle oplysninger og efterretninger, herunder personoplysninger, med henblik på udførelsen af sine opgaver; medlemsstaterne kan kun bruge oplysninger hentet fra Europols dataregistre med henblik på at forebygge og bekæmpe alvorlig grænseoverskridende kriminalitet. Enhver begrænsning, som en formidlende medlemsstat pålægger brugen af de videresendte oplysninger, gælder også andre brugere, som henter sådanne oplysninger fra Europols analyseregistre. Europol kan også udveksle personoplysninger med tredjelande, der har indgået operative aftaler med Europol og har et passende databeskyttelsesniveau. Europol kan kun lagre oplysninger, så længe de er nødvendige for udførelsen af enhedens opgaver. Analyseregistre må højst opbevares i en treårig periode, der dog kan forlænges med yderligere en treårig periode. Europols behandling af personoplysninger skal være i overensstemmelse med de specifikke regler for databeskyttelse i afgørelsen om oprettelse af Europol (Rådets afgørelse 2009/371/RIA) samt forordning (EF) nr. 45/2001, Europarådets konvention 108 med tillægsprotokol 181 og henstillingen om politiets brug af personoplysninger[63]. Bestemmelserne i Rådets

---

62 Rådets afgørelse 2009/371/RIA, EUT L 121 af 15.5.2009, der erstatter konventionen udarbejdet på grundlag af artikel K.3 i traktaten om Den Europæiske Union om oprettelse af en europæisk politienhed, EFT C 316 af 27.11.1995, s. 2.

63 Rådets afgørelse 2009/371/RIA, EUT L 121 af 15.5.2009, s. 37; forordning (EF) nr. 45/2001, EUT L 8 af 12.1.2001, s. 1; konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling (ETS nr. 108), Europarådet, 28.1.1981 (Europarådets konvention 108); tillægsprotokol til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af

rammeafgørelse 2008/977/RIA gælder for udveksling af personoplysninger mellem medlemsstaterne og Europol[64]. En fælles kontrolinstans, der består af medlemmer af nationale tilsynsorganer, overvåger Europols behandling af personoplysninger samt Europols formidling af personoplysninger til andre parter. Den fremlægger regelmæssige rapporter for Europa-Parlamentet og Rådet. Europol fremlægger en årsrapport om sine aktiviteter for Rådet til godkendelse og Europa-Parlamentet til orientering.

Ud over de følger for flere instrumenter, som er beskrevet ovenfor, førte terrorangrebene den 11. september 2001 til oprettelsen i 2002 af **Den Europæiske Enhed for Retligt Samarbejde** (Eurojust)[65]. Eurojust er et EU-organ, der har til formål at forbedre koordineringen af efterforskningen og retsforfølgningen i medlemsstaterne og fremme samarbejdet mellem medlemsstaternes kompetente myndigheder. Eurojust dækker de samme typer kriminalitet som Europol. Inden for rammerne af dette mandat og med henblik på udførelsen af deres opgaver har Eurojusts 27 nationale medlemmer, der udgør kollegiet, adgang til personoplysninger for mistænkte og lovovertrædere. Sådanne oplysninger omfatter bl.a. følgende: personoplysninger, kontaktoplysninger, oplysninger om køretøjsregistrering, DNA-profiler, fotografier, fingeraftryk, lokaliserings- og abonnentoplysninger fremlagt af udbydere af telekommunikationstjenester. Medlemsstaterne forventes at udveksle sådanne oplysninger med Eurojust for at give enheden mulighed for at udføre sine opgaver. Alle sagsrelaterede personoplysninger skal indlæses i Eurojusts automatiserede sagsforvaltnings-system, der anvender Kommissionens s-TESTA-netværk. Et indekssystem lagrer personlige og ikke-personlige oplysninger, der er relevante for igangværende undersøgelser. Eurojust kan behandle personoplysninger i forbindelse med udførelsen af sine opgaver, men sådanne operationer skal være i overensstemmelse med de specifikke regler i afgørelsen om oprettelse af Eurojust (Rådets afgørelse 2009/426/RIA), Europarådets konvention 108 med tillægsprotokol 181 og henstillingen om politiets brug af personoplysninger. Bestemmelserne i Rådets rammeafgørelse 2008/977/RIA gælder for udveksling af personoplysninger mellem medlemsstaterne og Eurojust[66]. Eurojust kan udveksle oplysninger med de nationale myndigheder og tredjelande, som der er indgået en aftale med, forudsat at det nationale medlem, der har givet oplysningerne, giver sit samtykke til en sådan videregivelse, og at tredjelandet sikrer en passende beskyttelse af personoplysningerne. Personoplysninger kan opbevares, så længe det er nødvendigt for at opfylde Eurojusts mål, men skal slettes, når en sag er afsluttet. Medlemsstaterne skal gennemføre Eurojusts ændrede retsgrundlag inden juni 2011. I juni 2014 skal Kommissionen revidere informationsudvekslingen mellem Eurojusts nationale medlemmer og eventuelt foreslå ændringer, den måtte finde nødvendige. I juni 2013 skal Eurojust rapportere til Rådet og Kommissionen om erfaringer med på nationalt niveau at give adgang til enhedens sagsforvaltningssystem. Medlemsstaterne kan på dette grundlag tage de nationale adgangsrettigheder op til revision. En fælles kontrolinstans, der består af dommere, som medlemsstaterne udnævner, overvåger Eurojusts behandling af personoplysninger og rapporter hvert år til Rådet. Formanden for Eurojust-kollegiet forelægger Rådet en årlig rapport om Eurojusts aktiviteter, som Rådet videresender Europa-Parlamentet.

---

personoplysninger, hvad angår tilsynsmyndigheder og overførsel af personoplysninger på tværs af grænserne (ETS nr. 181), Europarådet, 8.11.2001 (tillægsprotokol 181); Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, Europarådet, 17.9.1987.

64 Rådets rammeafgørelse 2008/977/RIA, EUT L 350 af 30.12.2008, s. 60.

65 Rådets afgørelse 2002/187/RIA, EFT L 63 af 6.3.2002, s. 1, ændret ved Rådets afgørelse 2009/426/RIA, EUT L 138 af 4.6.2009, s. 14. Ekstraordinært møde i Rådet (retlige og indre anliggender), 20.9.2001.

66 Rådets rammeafgørelse 2008/977/RIA, EUT L 350 af 30.12.2008, s. 60.

Internationale aftaler, der tager sigte på at forebygge og bekæmpe terrorisme og andre former for alvorlig grænseoverskridende kriminalitet

Efter terrorangrebet den 11. september 2001 vedtog USA lovgivning, der kræver, at flyselskaber, der flyver til, fra eller gennem USA's territorium, skal give de amerikanske myndigheder de **passagerlisteoplysninger** (Passenger Name Record, PNR), der er lagret i deres automatiske reservationssystemer. Umiddelbart efter besluttede Canada og Australien at indføre samme regler. Da den relevante EU-lovgivning kræver en forudgående vurdering af databeskyttelsesniveauet i tredjelande, trådte Kommissionen til og forhandlede PNR-aftaler med disse lande[67]. Den indgik aftalen med USA i juli 2007, med Australien i juni 2008 og en API/PNR-aftale med Canada i oktober 2005[68]. De amerikanske og australske aftaler finder midlertidig anvendelse, mens den canadiske forbliver i kraft, selv om Kommissionens beslutning om et tilstrækkeligt beskyttelsesniveau for de canadiske databeskyttelsesstandarder udløb i september 2009[69]. Europa-Parlamentet, som forholder sig kritisk til aftalernes indhold, har anmodet Kommissionen om at genforhandle alle tre aftaler på basis af klare principper[70]. PNR-oplysninger, der udveksles forud for et flys afgang, hjælper de retshåndhævende myndigheder med at tjekke passagerer for eventuelle forbindelser til terrorisme og andre former for alvorlig kriminalitet. Formålet med aftalerne er derfor at forebygge og bekæmpe terrorisme og andre former for alvorlig grænseoverskridende kriminalitet. Til gengæld for PNR-oplysninger fra EU udveksler det amerikanske ministerium for national sikkerhed (Department of Homeland Security, DHS) "spor", der følger af PNR-analysen, med EU's retshåndhævende myndigheder, Europol og Eurojust; og både Canada og USA har i deres respektive aftaler forpligtet sig til at samarbejde med EU om oprettelsen af EU's eget PNR-system. Den amerikanske og australske aftale indeholder 19 datakategorier, herunder personoplysninger og oplysninger om reservation og betaling og supplerende oplysninger; den canadiske aftale indeholder 25 lignende datakategorier. Disse supplerende oplysninger omfatter bl.a. oplysninger om enkeltbilletter, standby-status og "no show"-status. Den amerikanske aftale giver også mulighed for på visse betingelser at bruge følsomme oplysninger. DHS kan behandle sådanne oplysninger, hvis en registrerets eller andres liv er i fare, men skal slette dem inden for en frist på 30 dage. PNR-oplysninger sendes til centrale enheder i DHS, Canadas grænsekontrolmyndighed (Canada Border Services Agency) og de australske toldmyndigheder, og de må kun udveksles med andre nationale myndigheder med ansvar for retshåndhævelse og terrorbekæmpelse. I aftalen med USA forventer DHS, at det databeskyttelsesniveau, der vil blive anvendt i forbindelse med behandling af PNR-oplysninger fra EU "ikke vil være strengere", end det niveau EU-myndighederne anvender i deres nationale PNR-systemer. Hvis denne forventning ikke opfyldes, kan DHS suspendere visse dele af aftalen. EU mener, at Canada og Australien tilvejebringer et "passende" beskyttelsesniveau for PNR-oplysninger fra EU, hvis de opfylder betingelserne i deres respektive aftaler. I USA opbevares PNR-oplysninger fra EU i syv år i en aktiv database og

---

67 Direktiv 95/46/EF (databeskyttelsesdirektivet), EFT L 281 af 23.11.1995, s. 31.

68 Den canadiske pakke består af en canadisk forpligtelse vedrørende behandlingen af API/PNR-oplysninger, Kommissionens afgørelse om et tilstrækkeligt beskyttelsesniveau for de canadiske beskyttelsesstandarder og en international aftale (EUT L 91 af 29.3.2006, s. 49; EUT L 82 af 21.3.2006, s. 14). Aftalen med USA findes i EUT L 204 af 4.8.2007, s. 16; den australske aftale i EUT L 213 af 8.8.2008, s. 47.

69 I 2009 forpligtede Canada sig til over Kommissionen, Rådets formandskab og EU-medlemsstaterne fortsat at overholde de tidligere forpligtelser fra 2005 vedrørende brug af EU's PNR-oplysninger. Kommissionens beslutning om et tilstrækkeligt sikkerhedsniveau var baseret på denne tidligere fopligtelse.

70 Europa-Parlamentets beslutning, PT_TA(2010)0144 af 5.5.2010.

yderligere otte år i en inaktiv database. I Australien opbevares de i en aktiv base i 3,5 år og derefter i en inaktiv database i to år. I begge lande kræves der en særlig tilladelse for at søge i den inaktive database. I Canada opbevares oplysningerne i 3,5 år, dog således at oplysningerne gøres anonyme efter 72 timer. Hver aftale foreskriver regelmæssige revisioner, og den canadiske og australske aftale indeholder også en opsigelsesbestemmelse. I EU har kun Det Forenede Kongerige et PNR-system. Frankrig, Danmark, Belgien, Sverige og Nederlandene har enten vedtaget den nødvendige lovgivning eller er ved at teste bruge af PNR-oplysninger med henblik på indførelse af PNR-systemer. Flere andre medlemsstater overvejer at indføre PNR-systemer, og alle medlemsstater bruger fra sag til sag PNR-oplysninger med henblik på retshåndhævelse.

Efter terrorangrebet den 11. september 2001 udviklede det amerikanske finansministerium sit **program til sporing af finansiering af terrorisme** (Terrorist Finance Tracking Program, TFTP) for at identificere, spore og retsforfølge terrorister og deres finansielle støtter. I henhold til TFTP krævede det amerikanske finansministerium ved hjælp af administrative pålæg, at et belgisk selskab udleverede begrænsede sæt af oplysninger om finansielle transaktioner, der var foregået via dets netværk. I januar 2010 ændrede dette selskab sin systemarkitektur, hvilket mere end halverede den datamængde, der var under amerikansk jurisdiktion og typisk berørt af administrative pålæg. I november 2009 indgik formandskabet for Rådet for Den Europæiske Union og De Forenede Staters regering en interimsaftale om behandling og overførsel af finansielle betalingsdata fra EU til USA til brug for programmet til sporing af finansiering af terrorisme, som Europa-Parlamentet ikke godkendte[71]. På grundlag af et nyt mandat forhandlede Europa-Kommissionen et nyt udkast til aftale med USA og forelagde den 18. juni 2010 et forslag til Rådets afgørelse om indgåelse af aftalen 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 (TFTP-aftalen mellem EU og USA)[72]. Europa-Parlamentet godkendte indgåelsen af aftalen den 8. juli 2010[73]. Det forventes nu, at Rådet vedtager en afgørelse om indgåelse af aftalen, hvorefter aftalen kan træde i kraft gennem en brevudveksling mellem de to parter. Formålet med TFTP-aftalen mellem EU og USA er at forebygge, efterforske, afsløre og retsforfølge terrorisme eller finansiering heraf. Det forpligter udpegede leverandører af finansielle betalingstjenester til på basis af specifikke geografiske trusselsvurderinger og målrettede anmodninger at overføre finansielle betalingsdata til det amerikanske finansministerium, der bl.a. skal indeholde navn, kontonummer, adresse og id-nummer for ordregiver og begunstiget(begunstigede) for de finansielle transaktioner. Finansministeriet må kun anmode om sådanne oplysninger med henblik på TFTP, og kun hvis der er grund til at formode, at en identificeret person har en forbindelse til terrorisme eller finansiering heraf. Data mining og overførsel af data vedrørende transaktioner i det fælleseuropæiske betalingsområde er forbudt. USA forsyner EU-medlemsstaterne, Europol og Eurojust med "spor" vedrørende potentielle terrorhandlinger i EU og vil hjælpe EU med at indføre sit eget system i lighed med TFTP. Hvis EU indfører et sådant program, er det muligt, at de to parter revurderer aftalen. Før der kan overføres data, skal alle anmodninger fra USA kontrolleres af Europol for at sikre, at de opfylder aftalens betingelser. Oplysninger udtrukket af finansielle betalingsdata må ikke opbevares længere, end det er nødvendigt for den specifikke efterforskning eller retsforfølgning; ikke-udtrukne oplysninger kan højst opbevares i 5 år. Når det er nødvendigt af hensyn til efterforskning,

---

71 Europa-Parlamentets beslutning, PT_TA(2010)0144 af 11.2.2010.

72 KOM(2010) 316 endelig/2 af 18.6.2010.

73 Europa-Parlamentets beslutning P7_TA-PROV(2010)0279, af 8.7.2010.

forebyggelse eller retsforfølgning af terrorisme eller finansiering heraf, kan finansministeriet overføre personoplysninger udtrukket af finansielle betalingsdata til amerikanske retshåndhævende myndigheder, offentlige sikkerhedsmyndigheder og terrorbekæmpende myndigheder, EU's medlemsstater, Europol eller Eurojust. Det kan også udveksle eventuelle spor med tredjelande vedrørende EU-borgere og personer med bopæl i EU, hvis den pågældende medlemsstat giver sit samtykke. Parternes overholdelse af aftalens klare terrorbekæmpende formålsbegrænsning og andre sikkerhedsforanstaltninger kontrolleres af uafhængige personer, herunder en person udpeget af Kommissionen. Den har en varighed på fem år, og begge parter kan opsige eller suspendere aftalen. Et EU-revisionsteam under Kommissionens ledelse og med repræsentanter for to databeskyttelsesmyndigheder og en jurist vil revidere aftalen seks måneder efter dens ikrafttrædelse og navnlig vurdere parternes overholdelse af formålsbegrænsningen og proportionalitetsbestemmelserne og overensstemmelse med deres databeskyttelsesforpligtelser. Kommissionens rapport vil blive forelagt Europa-Parlamentet og Rådet.

2.2. Initiativer under handlingsplanen for Stockholmprogrammet

Lovgivningsforslag, som Kommissionen skal fremlægge

I Stockholmprogrammet anmodede Det Europæiske Råd Kommissionen om at fremlægge tre forslag, der direkte vedrører denne meddelelse: et PNR-system for EU med henblik på forebyggelse, afsløring og retsforfølgning af terrorhandlinger og alvorlig kriminalitet, et ind- og udrejsesystem og et program til registrering af rejsende. Det Europæiske Råd opfordrede til, at de to sidstnævnte initiativer blev forelagt "snarest muligt". Kommissionen har indarbejdet alle tre anmodninger i sin handlingsplan for Stockholmprogrammet[74]. Den vil nu bestræbe sig på at gennemføre disse initiativer og fremover evaluere disse instrumenter på basis af principperne for politikudformning, der fremgår af afsnit 4.

I november 2007 fremlagde Kommissionen et forslag til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse[75]. Initiativet fik støtte i Rådet, og det blev efterfølgende ændret for at tage højde for Europa-Parlamentets ændringsforslag og synspunkter fremsat af den europæiske tilsynsførende for databeskyttelse. Med Lissabontraktatens ikrafttrædelse bortfaldt det. Som nævnt i handlingsplanen for Stockholmprogrammet arbejder Kommissionen nu på i begyndelsen af 2011 at kunne fremlægge en **passagerlistepakke** bestående af følgende: en meddelelse om en EU-ekstern PNR-strategi, der indeholder de hovedprincipper, som er vejledende for forhandling af aftaler med tredjelande, forhandlingsdirektiver for en genforhandling af PNR-aftaler med USA og Australien og forhandlingsdirektiver for en ny aftale med Canada. Kommissionen er ligeledes ved at udarbejde et nyt PNR-forslag for EU.

I 2008 fremsatte Kommissionen en række forslag for at udvikle EU's integrerede grænseforvaltning ved at lette tredjelandsstatsborgeres ind- og udrejse, samtidig med at den indre sikkerhed fremmes[76]. Meddelelsen, der behandlede dette spørgsmål konstaterede, at personer, der bliver længere, end de har tilladelse til, udgør den største gruppe ulovlige indvandrere i EU, og den foreslog eventuelt at indføre et ind- og udrejsesystem for tredjelandsstatsborgere, der indrejser i EU med henblik på kortvarige ophold af højst tre

---

74 Stockholmprogrammet - Et åbent og sikkert Europa i borgernes tjeneste og til deres beskyttelse, Rådets dokument 5731/10 af 3.3.2010. KOM(2010) 171 af 20.4.2010 (Stockholmprogrammets handligsplan).

75 KOM(2007) 654 af 6.11.2007.

76 KOM(2008) 69 af 13.2.2008.

måneders varighed. Et sådant system kan omfatte registrering af oplysninger om dato og sted for indrejsen, længden af det tilladte ophold og videresendelse af automatiske advarsler til de kompetente myndigheder, hvis der findes frem til en person, der er blevet længere, end den pågældende har tilladelse til. Baseret på en kontrol af biometriske data vil systemet kunne anvende samme biometriske matchsystem og driftsudstyr som SIS II og VIS. Kommissionen gennemfører i øjeblikket en konsekvensanalyse, og som det er nævnt i handlingsplanen for Stockholmprogrammet, vil den bestræbe sig på at fremlægge et lovgivningsforslag i 2011.

Et **program vedrørende personer med status som registreret rejsende** (Registered Travellers Programme, RTP) var det tredje forslag, der skulle overvejes[77]. Dette program ville give visse grupper af hyppigt rejsende tredjelandsstatsborgere mulighed for at indrejse i EU, under forudsætning af den nødvendige forudgående kontrol og under anvendelse af forenklet kontrol ved automatiske kontrolposter. RTP vil også blive baseret på identitetskontrol ved brug af biometriske data og give mulighed for gradvis at gå fra den nuværende generelle kontroltilgang til en tilgang baseret på individuel risiko. Kommissionen har foretaget en konsekvensanalyse, og forventer i overensstemmelse med Stockholmprogrammet at fremlægge et lovgivningsforslag i 2011.

Initiativer, som Kommissionen skal undersøge

I Stockholmprogrammet opfordrede Det Europæiske Råd Kommissionen til at undersøge tre initiativer, der vedrører denne meddelelse, nemlig mulighederne for at spore terrorfinansiering inden for EU, muligheden og nytten af at udvikle et europæisk system for rejsetilladelser og behovet for og merværdien ved at indføre et europæisk strafferegisterindekssystem. Kommissionen har indarbejdet alle tre initiativer i sin handlingsplan for Stockholm-programmet. Den vil nu vurdere muligheden for at gennemføre dem og beslutte, om og hvordan der kan gås videre på basis af principperne for politikudformning, der fremgår af afsnit 4.

TFTP-aftalen mellem EU og USA opfordrer Europa-Kommissionen til at undersøge en eventuel indførelse af et **EU-system til sporing af finansiering af terrorisme** svarende til USA's TFTP, der kan give mulighed for en "mere målrettet" overførsel af data fra EU til USA. Udkastet til Rådets afgørelse om indgåelse af denne aftale opfordrer også Kommissionen til senest et år efter ikrafttrædelsen af TFTP-aftalen mellem EU og USA at forelægge Europa-Parlamentet og Rådet en juridisk og teknisk ramme for udtræk af data på EU's område[78]. Senest tre år efter denne aftales ikrafttrædelse skal Kommissionen fremlægge en statusrapport om udviklingen af et sådant tilsvarende EU-system. Hvis der ikke senest fem år efter aftalens ikrafttrædelse er indført et sådant system, kan EU beslutte at opsige aftalen. TFTP-aftalen mellem EU og USA forpligter også USA til at samarbejde med EU og yde bistand og rådgivning, hvis EU skulle beslutte at indføre et sådant system. Uden at det berører en eventuel beslutning, er Kommissionen begyndt at overveje databeskyttelse og de ressourcemæssige og praktiske følger af dette initiativ. Som nævnt i handlingsplanen for Stockholmprogrammet vil Kommissionen i 2011 fremlægge en meddelelse om muligheden for at indføre et EU-program til sporing af finansiering af terrorisme (TFTP på EU-niveau).

---

77 KOM(2008) 69 af 13.2.2008.

78 Rådets dokument 11222/1/10, REV1 af 24.6.2010; Rådets dokument 11222/1/10, REV1 COR1 af 24.6.2010.

I meddelelsen fra 2008 om integreret grænseforvaltning foreslog Kommissionen eventuelt at indføre et **elektronisk system for rejsetilladelser** (ESTA) for tredjelandsstatsborgere, der ikke er visumpligtige[79]. I henhold til dette program vil de berørte tredjelandsstatsborgere blive anmodet om forud for deres rejse at udarbejde en elektronisk ansøgning med personoplysninger og pas- og rejseoplysninger. Sammenlignet med visumproceduren vil ESTA gøre det muligt hurtigere og enklere at kontrollere, om en person opfylder de nødvendige indrejsebetingelser. Kommissionen foretager i øjeblikket en undersøgelse af fordele, ulemper og praktiske følger af en indførelse af ESTA. Som nævnt i handlingsplanen for Stockholmprogrammet er det Kommissionens hensigt i 2011 at fremlægge en meddelelse om muligheden for at indføre et sådant program.

Tyskland indledte under sit formandskab i 2007 en drøftelse om en eventuel indførelse af et **europæisk strafferegisterindekssystem** (EPRIS)[80]. EPRIS skal hjælpe de retshåndhævende myndigheder med at lokalisere oplysninger i EU, navnlig vedrørende forbindelser mellem personer, der mistænkes for organiseret kriminalitet. Kommissionen vil i 2010 fremlægge sit udkast til kommissorium for gennemførlighedsundersøgelsen vedrørende EPRIS. Som nævnt i handlingsplanen for Stockholmprogrammet er det Kommissionens hensigt i 2012 at fremlægge en meddelelse om muligheden for at indføre et sådant system.

3. ANALYSE AF INSTRUMENTER, DER ANVENDES, ER VED AT BLIVE GENNEMFØRT ELLER OVERVEJES

Ovennævnte oversigt giver anledning til følgende foreløbige bemærkninger:

Decentraliseret struktur

Kun seks af de forskellige instrumenter, der på nuværende tidspunkt anvendes, er ved at blive gennemført eller overvejes, medfører indsamling eller lagring af personoplysninger på EU-niveau, nemlig SIS (og SIS II), VIS, EURODAC, CIS, Europol og Eurojust. Alle de andre foranstaltninger regulerer den decentraliserede, grænseoverskridende udveksling eller overførsel til tredjelande af personoplysninger, som er indsamlet på nationalt niveau af offentlige myndigheder eller private selskaber. De fleste personoplysninger indsamles og lagres nationalt. EU forsøger at skabe merværdi ved på visse betingelser at muliggøre udveksling af sådanne oplysninger med EU-partnere og tredjelande. Kommissionen har netop forelagt Europa-Parlamentet og Rådet et ændret forslag om oprettelse af et agentur for den operationelle forvaltning af store it-systemer inden for området frihed, sikkerhed og retfærdighed[81]. Det kommende it-agenturs opgave vil være at varetage de operationelle forvaltningsopgaver for SIS II, VIS og Eurodac og andre kommende it-systemer inden for området frihed, sikkerhed og retfærdighed og sørge for, at systemerne fungerer døgnet rundt alle ugens syv dage, så der sikres en kontinuerlig, uafbrudt udveksling af oplysninger.

Begrænset formål

De fleste af de ovenfor analyserede instrumenter har et specifikt formål: EURODAC skal fremme Dublin-systemets drift; API-systemet skal forbedre grænsekontrollen; det svenske initiativ skal fremme strafferetlig efterforskning og efterretningsoperationer;

---

79 KOM(2008) 69 af 13.2.2008.

80 Se Rådets dokument 15526/1/09 af 2.12.2009.

81 KOM(2010) 93 af 19.3.2010.

Napoli II-konventionen skal bidrage til at forebygge, afsløre, retsforfølge og straffe toldsvig; CIS skal bistå med at forebygge, efterforske og retsforfølge alvorlige overtrædelser af den nationale toldlovgivning ved at sikre et mere effektivt samarbejde mellem de nationale toldmyndigheder; ECRIS, FIU og ARO skal strømline grænseoverskridende udveksling af oplysninger på særlige områder, og Prümafgørelsen, datalagringsdirektivet, TFTP og PNR skal bekæmpe terrorisme og alvorlig kriminalitet. SIS, SIS II og VIS er hovedundtagelserne fra dette mønster. Det oprindelige formål med VIS var at fremme grænseoverskridende udveksling af visumoplysninger, men det blev efterfølgende udvidet til også at omfatte forebyggelse og bekæmpelse af terrorisme og alvorlig kriminalitet. SIS og SIS II har til formål at sikre et højt sikkerhedsniveau på området frihed, sikkerhed og retfærdighed og fremme borgernes bevægelighed ved at bruge oplysninger, der udveksles via dette system. Med undtagelse af disse centraliserede informationssystemer synes formålsbegrænsning at være en afgørende faktor for udviklingen af informationsstyringssystemer på EU-niveau.

Mulige overlapninger

De samme personoplysninger kan indsamles via flere forskellige instrumenter, men kan kun bruges til et begrænset formål inden for rammerne af et bestemt instrument (bortset fra VIS, SIS og SIS II). F.eks. kan oplysninger om en person, herunder navn, fødselsdato og -sted og nationalitet behandles via SIS, SIS II, VIS, API, CIS, det svenske initiativ, Prümafgørelsen, ECRIS, FIU'er, ARO'er, Europol, Eurojust og PNR- og TFTP-aftaler. Sådanne oplysninger kan imidlertid kun behandles med henblik på grænsekontrol inden for rammerne af API; forebyggelse, efterforskning og retsforfølgning af toldsvig inden for rammerne af CIS; strafferetlig efterforskning og efterretningsoperationer inden for rammerne af det svenske initiativ; forebyggelse af terrorisme og grænseoverskridende kriminalitet inden for rammerne af Prümafgørelsen; undersøgelse af en persons kriminelle baggrund inden for rammerne af ECRIS; undersøgelse af en persons forbindelser med organiseret kriminalitet og terrornetværk inden for rammerne af FIU'er; sporing af aktiver inden for rammerne af ARO'er; efterforskning og bistand med retsforfølgning af grænseoverskridende kriminalitet, hvad angår Europol og Eurojust; forebyggelse og bekæmpelse af terrorisme og andre former for alvorlig grænseoverskridende kriminalitet for PNR's vedkommende; identifikation og retsforfølgning af terrorister og deres finansiering for TFTP's vedkommende. Biometriske data, som f.eks. fingeraftryk og billeder, kan behandles inden for rammerne af SIS II, VIS, EURODAC, det svenske initiativ, Prümafgørelsen, ECRIS, Europol og Eurojust – men også i dette tilfælde inden for rammerne af det afgrænsede formål med hvert enkelt instrument. Prümafgørelsen er det eneste instrument, der giver mulighed for grænseoverskridende udveksling af anonyme DNA-profiler (selv om sådanne oplysninger også kan fremsendes til Europol og Eurojust). Andre foranstaltninger behandler højt specialiserede personoplysninger, som er relevante for deres anvendelsesområde: PNR-systemer behandler flypassager-oplysninger; FIDE behandler oplysninger vedrørende efterforskning af toldsvig; datalagrings-direktivet vedrører IP-adresser og brugeridentitet; ECRIS strafferegistre; ARO private aktiver og selskabsoplysninger; it-platforme, internetovertrædelser; Europol forbindelser til kriminelle netværk og TFTP finansielle betalingsdata. Den grænseoverskridende udveksling af oplysninger og efterretninger til strafferetlig efterforskning er det eneste eksempel på en egentlig overlapning. Fra et juridisk synspunkt ville det svenske initiativ være tilstrækkeligt til at udveksle alle typer oplysninger af betydning for en sådan efterforskning (forudsat at udvekslingen af sådanne personoplysninger er tilladt ifølge national lovgivning). Fra et operationelt synspunkt kan Prümafgørelsen være at foretrække for udveksling af DNA-profiler og fingeraftryksoplysninger, da dens system med "hit/ikke-hit" giver et øjeblikkeligt svar, og dens metode til automatisk udveksling af oplysninger sikrer et højt

databeskyttelsesniveau[82]. På samme måde kan det være mere effektivt for FIU'er, ARO'er og it-kriminalitetsplatforme at samarbejde direkte med deres kolleger i EU uden at skulle udfylde de formularer, der kræves ifølge det svenske initiativ for at anmode om oplysninger.

Kontrollerede adgangsrettigheder

Adgangsrettigheder for instrumenter, der er indført med henblik på bekæmpelse af terrorisme og alvorlig kriminalitet gives normalt kun til visse retshåndhævende myndigheder, nemlig politi, grænsekontrolmyndigheder og toldmyndigheder. Adgangsrettigheder til Schengen-instrumenterne gives typisk til indvandringsmyndigheder og på visse betingelser politi, grænsekontrolmyndigheder og toldmyndigheder. Informationsstrømmen kontrolleres af nationale grænseflader, hvad angår de centraliserede SIS og VIS, og nationale kontaktpunkter eller centrale koordineringsenheder, hvad angår decentraliserede instrumenter, som f.eks. Prümafgørelsen, det svenske initiativ, Napoli II-konventionen, ECRIS, TFTP, PNR-aftaler, FIU'er, ARO'er og it-kriminalitetsplatforme.

Forskellige datalagringsregler

Datalagringsperioder varierer meget afhængig af de forskellige instrumenters formål. PNR-aftalen med USA har den længste datalagringsperiode – 15 år, mens API har den korteste – 24 timer. PNR-aftaler har en interessant sondring mellem data i aktiv og passiv brug. Efter en vis periode skal oplysninger nemlig arkiveres og kan kun "låses op" med særlig tilladelse. Den canadiske brug af EU's PNR-oplysninger giver et godt eksempel, idet oplysningerne skal gøres anonyme efter 72 timer, men er tilgængelige for godkendte medarbejdere i 3,5 år.

Effektiv identitetsforvaltning

Flere af ovennævnte foranstaltninger, herunder de kommende SIS II og VIS, skal give mulighed for identitetskontrol gennem brug af biometriske data. Gennemførelsen af SIS II forventes at fremme sikkerheden på området frihed, sikkerhed og retfærdighed ved f.eks. at hjælpe med at identificere personer, der er omfattet af en europæisk arrestordre, personer, der nægtes indrejse i Schengenområdet, og personer, der eftersøges af andre specifikke efterforskningsgrunde (som f.eks. forsvundne personer eller vidner i retssager) uanset identifikationspapirernes tilgængelighed eller ægthed. Gennemførelsen af VIS burde fremme visumudstedelses- og visumforvaltningsprocessen.

EU-løsninger for datasikkerhed

For udveksling af følsomme oplysninger inden for EU-grænser foretrækker medlemsstaterne EU-løsninger. Flere instrumenter af forskellig størrelse, struktur og med forskelligt formål bruger s-TESTA-netværket, som er finansieret af Kommissionen, til udveksling af følsomme oplysninger. Det gælder de centraliserede systemer SIS II, VIS og EURODAC, Prümafgørelsens decentrale instrument og de decentrale instrumenter ECRIS og FIU samt Europol og Eurojust. CIS og FIDE er baseret på Common Communication Network, Common System Interface eller sikker webadgang stillet til rådighed af Kommissionen. I

[82] Prümafgørelsen (Rådets afgørelse 2008/615/RIA, EUT L 210 af 6.8.2008, s. 1) har en tilsvarende gennemførelsesafgørelse (Rådets afgørelse 2008/616/RIA, EUT L 210 af 6.8.2008, s. 12), der tager sigte på at sikre brug af de seneste tekniske foranstaltninger for at sikre databeskyttelse og datasikkerhed samt krypterings- og godkendelsesprocedurer for adgang til data og omfatter særlige regler for søgningers lovlighed.

mellemtiden ser Europols netværksapplikation til informationsudveksling, SIENA, ud til at være blevet den foretrukne applikation for nogle af de seneste initiativer, der kræver sikker dataoverførsel. Der er drøftelser i gang om at lade FIU.net, ARO'er og it-kriminalitetsplatforme fungere på grundlag af denne applikation.

Forskellige revisionsmekanismer

Ovennævnte instrumenter indeholder en række forskellige revisionsmekanismer. I forbindelse med komplekse informationssystemer, som f.eks. SIS II, VIS og EURODAC skal Kommissionen forelægge Europa-Parlamentet og Rådet årlige eller halvårlige rapporter om driften eller gennemførelsessituationen for disse systemer. For decentrale informationsudvekslingsinstrumenters vedkommende skal Kommissionen forelægge de øvrige institutioner en evalueringsrapport nogle år efter gennemførelsen. Datalagrings-direktivet, det svenske initiativ og ARO-foranstaltningerne skal evalueres i 2010, Prümafgørelsen i 2012 og ECRIS i 2016. De tre PNR-aftaler foreskriver regelmæssige og ad hoc-revisioner, og to af dem indeholder også opsigelsesbestemmelser. Europol og Eurojust fremlægger årsrapporter for Rådet, der videresender dem til Europa-Parlamentet til orientering. Disse overvejelser antyder, at den nuværende struktur for informationsstyring i EU ikke er egnet til at vedtage en fælles evalueringsmekanisme for alle instrumenter. I betragtning af disse forskellige forhold er det vigtigt, at alle ændringer af instrumenter inden for informationsstyring tager højde for de potentielle følger for alle andre instrumenter, der regulerer indsamling, lagring eller udveksling af personoplysninger på området frihed, sikkerhed og retfærdighed.

4. PRINCIPPER FOR POLITIKUDFORMNING

Afsnit 2 beskrev flere initiativer, som Europa-Kommissionen har gennemført, fremlagt eller overvejet i de seneste år. Bare antallet af nye ideer og den stigende mængde lovgivning inden for intern sikkerhed og migrationsforvaltning gør det nødvendigt at definere et sæt grundlæggende principper, der skal være vejledende for iværksættelsen og evalueringen af initiativer i de kommende år. Disse principper bygger på og supplerer de generelle principper i EU-traktaterne, retspraksis for Den Europæiske Unions Domstol og Den Europæiske Menneskerettighedsdomstol og de relevante interinstitutionelle aftaler mellem Europa-Parlamentet, Rådet og Europa-Kommissionen. Kommissionen foreslår at udvikle og gennemføre nye initiativer og evaluere de nuværende instrumenter på basis af følgende to sæt principper:

Materielle principper

Beskytte de grundlæggende rettigheder, navnlig retten til respekt for privatliv og beskyttelse af personoplysninger

Beskyttelse af borgernes grundlæggende rettigheder som fastslået i Den Europæiske Unions charter om grundlæggende rettigheder, navnlig retten til respekt for privatliv og beskyttelse af personoplysninger vil være en prioritet for Kommissionen i forbindelse med udarbejdelse af nye forslag, der indebærer behandling af personoplysninger på området intern sikkerhed eller migrationsforvaltning. Artikel 7 og 8 i chartret fastslår, at "Enhver har ret til respekt for sit privatliv og familieliv" og til "beskyttelse af personoplysninger, der vedrører ham/hende"[83].

[83] Den Europæiske Unions charter om grundlæggende rettigheder, EUT C 83 af 30.3.2010, s. 389.

Artikel 16 i traktaten om Den Europæiske Unions funktionsmåde, som er bindende for medlemsstaternes aktiviteter, EU-institutionerne, agenturer og organer, fastslår, at enhver har ret til "beskyttelse af personoplysninger om vedkommende selv"[84]. Når der skal udvikles nye instrumenter, der er baseret på brug af informationsteknologi, vil Kommissionen forsøge at følge den tilgang, der kaldes "privacy by design" (indbygget databeskyttelse). Det betyder, at beskyttelse af personoplysninger skal indarbejdes i det teknologiske grundlag for et givet instrument, at databehandling skal begrænses til det, der er nødvendigt for at nå et givet mål, og at der kun gives adgang til oplysningerne til de enheder, der har "behov for at få kendskab" til oplysninger[85].

Nødvendighed

En offentlig myndigheds indblanden i enkeltpersoners ret til privatlivets fred kan være nødvendig af hensyn til den nationale sikkerhed, den offentlige orden eller forebyggelse af kriminalitet[86]. Den Europæiske Menneskerettighedsdomstols retspraksis fastslår tre betingelser for, at disse begrænsninger kan være begrundede: de skal være lovlige, have et lovligt formål og være nødvendige i et demokratisk samfund. Indgreb i retten til privatlivets fred betragtes som nødvendig, hvis det skyldes et presserende samfundsmæssigt behov, hvis det står i et rimeligt forhold til det forfulgte mål, og hvis de grunde, den offentlige myndighed anfører som begrundelse, er relevante og tilstrækkelige[87]. I alle kommende forslag vil Kommissionen vurdere initiativets forventede virkning for borgernes ret til privatlivets fred og beskyttelse af personoplysninger og gøre rede for, hvorfor en sådan virkning er nødvendig, og hvorfor den foreslåede løsning står i et rimeligt forhold til det legitime mål om at opretholde den indre sikkerhed i Den Europæiske Union, forebygge kriminalitet eller forvalte migration. Overensstemmelse med reglerne om beskyttelse af personoplysninger vil i alle tilfælde blive kontrolleret af en uafhængig myndighed på nationalt niveau eller EU-niveau.

Nærhedsprincippet

Kommissionen vil forsøge at begrunde sine nye forslag på baggrund af nærhedsprincippet og proportionalitetsprincippet i overensstemmelse med artikel 5 i protokol 2, der er tilknyttet traktaten om Den Europæiske Union. Alle nye lovgivningsmæssige forslag vil indeholde en analyse, der gør det muligt at vurdere overholdelsen af nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. Denne analyse vil indeholde en vurdering af forslagets finansielle, økonomiske og sociale virkninger, og når der er tale om et direktiv, følgerne for den lovgivning, som medlemsstaterne skal iværksætte[88]. Begrundelsen for at fastslå, at et af EU's mål bedre kan nås på EU-plan, vil blive underbygget af kvalitative indikatorer. Lovgivningsmæssige forslag vil tage i betragtning, at enhver byrde, der pålægges EU, nationale regeringer, regionale eller lokale myndigheder, erhvervsdrivende og borgere, skal begrænses mest muligt og stå i rimeligt forhold til det mål, der skal nås. Hvis der er tale om

---

84 Konsoliderede udgaver at traktaten om Den Europæiske Union og traktaten om Den Europæiske Unions funktionsmåde, EUT C 83 af 30.3.2010, s. 1.

85 For at få en samlet beskrivelse af "privacy by design" henvises der til udtalelse fra den europæiske tilsynsførende for databeskyttelse om styrkelse af tilliden til informationssamfundet ved at styrke databeskyttelsen og privatlivets fred, den europæiske tilsynsførende for databeskyttelse, 18.3.2010.

86 Se artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (ETS nr. 5), Europarådet, 4.11.1950.

87 Se *Marper mod Det Forenede Kongerige*, dom af 4.12.2008 afsagt af Den Europæiske Menneskerettighedsdomstol.

88 Grundprincipperne for konsekvensanalyser er fastsat i Europa-Kommissionens retningslinjer for konsekvensanalyser (SEK(2009) 92 af 15.1.2009).

forslag, der omhandler nye internationale aftaler, vil analysen undersøge forslagets forventede virkning for forbindelserne med de pågældende tredjelande.

Præcis risikostyring

Oplysninger på området frihed, sikkerhed og retfærdighed udveksles typisk for at analysere sikkerhedstrusler, identificere tendenser i den kriminelle aktivitet eller vurdere risici på dertil knyttede politikområder[89]. Risiko er ofte, men ikke nødvendigvis, knyttet til personer, hvis hidtidige adfærd eller adfærdsmønster antyder, at risikoen fortsat vil eksistere i fremtiden. Risici skal imidlertid vurderes på basis af beviser og ikke hypoteser. De nødvendige undersøgelser og den nødvendige formålsbegrænsning har afgørende betydning for alle foranstaltninger vedrørende informationsstyring. Udarbejdelse af risikoprofiler – der ikke må forveksles med racemæssige eller andre diskriminerende profiler, som er uforenelige med de grundlæggende rettigheder, er relevante. Sådanne profiler kan bidrage til at fokusere ressourcerne på særlige individer med henblik på at identificere sikkerhedstrusler og beskytte ofre for kriminalitet.

Procesorienterede principper[90]

Omkostningseffektivitet

Offentlige tjenester baseret på informationsteknologi bør gøre det muligt at sikre bedre tjenester og større værdi for skatteydernes penge. I betragtning af det nuværende økonomiske klima, vil alle nye forslag, navnlig når de vedrører indførelse eller opgradering af informationssystemer, være så omkostningseffektive som muligt. En sådan tilgang vil tage højde for allerede eksisterende løsninger for at mindske overlapning og øge mulige synergier. Kommissionen vil vurdere, om det er muligt at opfylde et forslags målsætninger gennem en bedre brug af allerede eksisterende instrumenter. Den vil også overveje at tilføje nye funktioner til eksisterende informationssystemer, før der foreslås nye systemer.

Bottom-up-politikudformning

Udviklingen af nye initiativer skal så tidligt som muligt trække på input fra alle relevante aktører, herunder nationale myndigheder med ansvar for gennemførelse, økonomiske aktører og civilsamfundet. At udforme politikker, der tager højde for slutbrugernes interesser, kræver tværfaglige overvejelser og omfattende høringer[91]. Af den grund vil Kommissionen forsøge at indføre faste forbindelser til nationale embedsmænd og aktører via Rådets strukturer, forvaltningskomitéer og ad hoc-strukturer.

Klar ansvarsfordeling

I betragtning af den tekniske kompleksitet for informationsindsamling og udvekslings-projekter på området frihed, sikkerhed og retfærdighed, skal der lægges særlig vægt på den

---

89 Som praktiske eksempler på succesrig risikostyring kan nævnes, at man forhindrede en udvist person, som havde begået en alvorlig forbrydelse i en medlemsstat fra at indrejse i Schengenområdet via en anden medlemsstat (SIS), eller at det blev forhindret, at en person indgav asylansøgning i flere medlemsstater (EURODAC).

90 Disse principper er baseret på Rådets konklusioner om en informationsstyringsstrategi for EU's indre sikkerhed, Rådet (retlige og indre anliggender) den 30.11.2009.

91 De generelle principper og minimumsstandarder ved Kommissionens høring af interesserede parter findes i KOM(2002) 704 af 11.12.2002.

indledende udformning af forvaltningsstrukturer. Erfaringen med SIS II-projektet viser, at hvis der ikke tidligt defineres klare og stabile overordnede mål, roller og ansvarsområder, kan det føre til betydelig budgetoverskridelser og forsinkelser i gennemførelsesfasen. En tidlig vurdering af erfaringen med gennemførelsen af Prümafgørelsen viser, at en decentraliseret forvaltningsstruktur heller ikke nødvendigvis er løsningen, da medlemsstaterne ikke har en projektleder at henvende sig til for at få råd om de finansielle og tekniske aspekter af gennemførelsen. Det kommende it-agentur vil kunne yde en sådan teknisk rådgivning til de ansvarlige for informationssystemer på området frihed, sikkerhed og retfærdighed. Det kan også tilbyde en platform og sikre, at aktørerne deltager talrigt i it-systemernes operationelle forvaltning og udvikling. For i så høj grad som muligt at undgå budgetoverskridelser og forsinkelser, der skyldes ændrede krav, vil nye informationssystemer på området frihed, sikkerhed og retfærdighed, navnlig hvis der er tale om et stort it-system, ikke blive udviklet, før de grundlæggende retlige instrumenter, der fastsætter formål, anvendelsesområde, funktioner og tekniske detaljer, er endelig vedtaget.

Bestemmelser om revision og ophør

Kommissionen vil evaluere alle instrumenter, der er omhandlet i denne meddelelse. Det vil ske på baggrund af de mange instrumenter, der findes på området informationsstyring. Det skulle give et pålideligt billede af, hvordan individuelle instrumenter passer ind i det store billede for intern sikkerhed og migrationsforvaltning. Kommende forslag vil eventuelt omfatte en årlig rapporteringsforpligtelse, regelmæssige og ad hoc-revisioner samt en bestemmelse om ophør. Eksisterende instrumenter vil kun blive bevaret, hvis de fortsat tjener det legitime formål, de blev udformet til. Bilag II indeholder revisionsdatoer og -mekanismer for hvert enkelt instrument i denne meddelelse.

5. VEJEN FREM

Denne meddelelse giver for første gang et klart og fuldstændigt overblik over foranstaltninger på EU-niveau, der allerede eksisterer eller er ved at blive gennemført eller udarbejdet, og som regulerer indsamling, lagring og grænseoverskridende udveksling af personoplysninger med henblik på retshåndhævelse og migrationsforvaltning.

Den giver borgerne et overblik over, hvilke oplysninger der indsamles, lagres eller udveksles, til hvilket formål og af hvem. Det er et referenceværktøj for aktører, der ønsker at deltage i debatten om, hvilken retning EU's politik på dette område skal tage. Samtidig giver den et første svar på Det Europæiske Råds opfordring til at udvikle informationsstyringssystemer på EU-niveau i overensstemmelse med EU's informationsstyringsstrategi[92] og til at overveje behovet for at udvikle en europæisk model for informationsudveksling[93].

Det er Kommissionens hensigt at følge op på denne meddelelse og fremlægge en meddelelse om en europæisk model for informationsudveksling[94]. I den henseende lancerede Kommissionen en "informationskortlægning" i januar 2010 om retsgrundlag og den praktiske

---

92 Rådets konklusioner om en informationsstyringsstrategi for EU's indre sikkerhed, Rådet (retlige og indre anliggender), 30.11.2009 (EU-informationsstyringsstrategi).

93 Stockholmprogrammet - Et åbent og sikkert Europa i borgernes tjeneste og til deres beskyttelse, Rådets dokument 5731/10 af 3.3.2010, afsnit 4.2.2.

94 Det fremgår af Kommissionens handlingsplan for Stockholmprogrammet (KOM(2010) 171 af 20.4.2010).

udveksling af strafferetlige efterretninger og oplysninger, og Kommissionen forventes at fremlægge resultaterne herfra for Rådet og Europa-Parlamentet i 2011[95].

Endelig fremsætter Kommissionen for første gang i denne meddelelse sin vision for de generelle principper, som den har til hensigt at følge i den fremtidige udvikling af instrumenter til dataindsamling, lagring og udveksling. Disse principper vil også blive brugt ved evalueringen af eksisterende instrumenter. Vedtagelse af en sådan principbaseret tilgang til politikudformning og evaluering forventes at gøre nuværende og kommende instrumenter mere sammenhængende og effektive på en måde, der fuldt ud overholder borgernes grundlæggende rettigheder.

[95] Denne informationskortlægningsøvelse udføres i tæt samarbejde med et ad hoc-hold bestående af repræsentanter for EU- og EFTA-medlemsstaterne, Europol, Eurojust, Frontex og den europæiske tilsynsførende for databeskyttelse.

BILAG I

Følgende data og eksempler har til formål at illustrere, hvordan de foranstaltninger, der på nuværende tidspunkt er gennemført, fungerer i praksis.

Schengeninformationssystemet (SIS)

Samlet antal SIS-indberetninger i den centrale SIS-database (C.SIS)[96]

Kategorier af indberetninger	**2007**	**2008**	**2009**
Pengesedler	177 327	168 982	134 255
Uudfyldte dokumenter	390 306	360 349	341 675
Skydevåben	314 897	332 028	348 353
Udstedte dokumenter	17 876 227	22 216 158	25 685 572
Køretøjer	3 012 856	3 618 199	3 889 098
Eftersøgte personer (med kaldenavn)	299 473	296 815	290 452
Eftersøgte personer (vigtigste navn)	859 300	927 318	929 546
Heraf:			
Personer, der begæres anholdt med henblik på udlevering	19 119	24 560	28 666
Tredjelandsstatsborgere på listen over personer, der skal nægtes indrejse	696 419	746 994	736 868
Savnede voksne personer	24 594	23 931	26 707
Savnede mindreårige	22 907	24 628	25 612
Vidner eller andre indkaldte	64 684	72 958	78 869
Personer, der er genstand for ekstraordinær overvågning for at forebygge trusler mod den offentlige orden	31 568	34 149	32 571
Personer, der er genstand for ekstraordinær overvågning for at forebygge trusler mod den nationale sikkerhed	9	98	253
I alt	**22 933 370**	**27 919 849**	**31 618 951**

[96] Rådets dokument 6162/10 af 5.2.2010; Rådets dokument 5764/09 af 28.1.2009; Rådets dokument 5441/08 af 30.1.2008.

Eurodac – Migrationsbevægelser blandt asylansøgere, som har indgivet nye ansøgninger i samme eller andre medlemsstater (2008)

Medlemsstater, der sender fingeraftryk med henblik på sammenligning og får hit fra medlemsstater (kolonnerne), hvor en person tidligere har ansøgt om visum	Medlemsstat, hvor den første asylansøgning blev indgivet[97]																													Samlet antal andengangs-ansøgninger	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	**Hit i hjemlandet**	**Hit i alt**
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8,129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1,341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1,759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**
Førstegangs-ansøgninger i alt	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

[97] KOM(2009) 494 af 25.9.2009. "Hit i hjemlandet" henviser til, at der er indgivet en ny asylansøgning i den medlemsstat, hvor den tidligere blev indgivet.

API-systemet (Advanced Passenger Information)

Det Forenede Kongeriges brug af API-oplysninger til forbedring af grænsekontrollen og bekæmpelse af ulovlig migration[98]	
Antal foranstaltninger i 2009	
Tidligere tilfælde af afslag (afslag på indrejse)	379
Bortkomne, stjålne eller annullerede pas (beslaglagt dokument)	56

[98] Kommissionen modtog disse oplysninger fra Det Forenede Kongeriges grænseagentur med henblik på denne meddelelse.

Toldinformationssystemet (CIS)

Samlet antal sager, der er indlæst i CIS-databasen (2009)[99]	
Foranstaltning	**CIS (baseret på CIS-konventionen)**
Oprettede sager	2 007
Aktive sager	274
Sager, hvortil der har været anmodninger om oplysninger	11 920
Slettede sager	1 355

[99] Oplysningerne stammer fra Kommissionen.

Svensk initiativ

Eksempler på brugen af det svenske initiativ til at efterforske forbrydelser[100]	
Manddrab	I 2009 fandt der et drabsforsøg sted i en medlemsstats hovedstad. Politiet indsamlede en biologisk prøve fra et glas, som den mistænkte havde drukket af. Ved at udtrække dna af denne prøve kunne retsmedicinerne generere en dna-profil. En sammenligning af denne profil med andre referenceprofiler i den nationale dna-database gav ikke noget match. Efterforskningspolitiet sendte derfor via deres Prümkontaktpunkt en anmodning om sammenligning af deres dna-referenceprofil med dem, andre medlemsstater, som er bemyndiget til at udveksle sådanne data på grundlag af Prümafgørelsen eller Prümaftalen, lå inde med. Denne sammenligning på tværs af grænserne gav et hit. På grundlag af det svenske initiativ anmodede efterforskningspolitiet om yderligere oplysninger om den mistænkte. Deres nationale kontaktpunkt modtog inden 36 timer svar fra flere andre medlemsstater, hvilket satte politiet i stand til at identificere den mistænkte.
Voldtægt	I 2003 voldtog en uidentificeret mistænkt en kvinde. Politiet indsamlede prøver fra ofret, men den dna-profil, der blev genereret fra prøven, matchede ikke nogen referenceprofil i den nationale dna-database. En anmodning om sammenligning af dna, som Prümkontaktpunktet sendte til andre medlemsstater, der var bemyndiget til at udveksle dna-referenceprofiler på grundlag af Prümafgørelsen eller Prümaftalen, gav et hit. Efterforsknings-politiet anmodede derefter om yderligere oplysninger om den mistænkte inden for rammerne af det svenske initiativ. Deres nationale kontaktpunkt modtog svar inden 8 timer, hvilket satte politiet i stand til at identificere den mistænkte.

[100] Kommissionen modtog disse eksempler fra en medlemsstats politistyrke med henblik på denne meddelelse.

Tyskland har opnået hit ved sammenligning på tværs af grænserne af dna-profiler efter type overtrædelse (2009)[101]

Hit efter type lovovertrædelse	Østrig	Spanien	Luxembourg	Neder-landene	Slovenien
Almenskadelige lovovertrædelser	32	4	0	5	2
Forbrydelser mod den personlige frihed	9	3	5	2	0
Seksualforbrydelser	40	22	0	31	4
Forbrydelser mod liv og legeme	49	24	0	15	2
Andre lovovertrædelser	3 005	712	18	1 105	71

[101] Den tyske regerings svar på parlamentsspørgsmål stillet af Ulla Jelpke, Inge Höger og Jan Korte (reference nr. 16/14120), Forbundsdagen, 16. møde, reference nr. 16/14150, 22.10.2009. Disse tal vedrører den periode, hvor en medlemsstat begyndte at udveksle data med Tyskland og sluttede den 30.9.2009.

Datalagringsdirektivet

Eksempler på medlemsstater, der opsporer alvorlige forbrydelser ved hjælp af lagrede data[102]	
Manddrab under skærpende omstændigheder	Det lykkedes for en medlemsstats politimyndigheder at opspore en gruppe drabsmænd, der var ansvarlige for racemotiverede drab på seks personer. Gerningsmændene forsøgte at undslippe ved at udskifte deres SIM-kort, men deres opkaldslister og mobiltelefonapparaternes identifikatorer.
Manddrab	Det lykkedes for en politimyndighed at bevise, at to mistænkte var involveret i manddrab ved at analysere datatrafikken fra ofrets mobiltelefon. Det gjorde det muligt for efterforskerne at rekonstruere den rute, som ofret og de to mistænkte var rejst ad sammen.
Indbrud	Myndighederne opsporede en gerningsmand, der var ansvarlig for 17 indbrud ved at undersøge datatrafikken fra den pågældendes anonyme forudbetalte SIM-kort. Ved at identificere den pågældendes kæreste fandt de også frem til gerningsmanden.
Svig	Efterforskere afslørede et svindelnummer, hvor en bande, der på internettet annoncerede med "kontantsalg" af dyre biler, systematisk berøvede de personer, der mødte frem for at overtage den bil, de havde købt. Ved hjælp af en IP-adresse lykkedes det politiet at opspore annoncøren og arrestere gerningsmændene.

[102] Disse anonyme eksempler er baseret på medlemsstaternes besvarelse af et spørgeskema fra Kommissionen i 2009 vedrørende gennemførelsen af direktiv 2006/24/EF (datalagringsdirektivet).

Samarbejde inden for rammerne af den finansielle efterretningsenhed (FIU)

Antal anmodninger om oplysninger fra nationale finansielle efterretningsenheder via FIU.net[103]		
År	**Anmodninger om oplysninger**	**Aktive brugere**
2007	3 133	12 medlemsstater
2008	3 084	13 medlemsstater
2009	3 520	18 medlemsstater

[103] Kommissionen modtog disse oplysninger fra FIU.net med henblik på denne meddelelse.

ARO-samarbejdet (samarbejdet mellem medlemsstaternes kontorer for inddrivelse af aktiver)

Anmodninger fra medlemsstaterne om opsporing af aktiver, som Europol behandlede[104]

År	**2004**	**2005**	**2006**	**2007**
Anmodninger	5	57	53	133
Heraf:				
Sager vedrørende svig				29
Sager vedrørende hvidvaskning af penge				26
Sager vedrørende narkotikahandel				25
Sager vedrørende andre overtrædelser				18
Sager vedrørende narkotikahandel og hvidvaskning af penge				19
Sager vedrørende svig og hvidvaskning af penge				7
Sager vedrørende forskellige overtrædelser				9

Sager om konfiskation af aktiver, som Eurojust behandlede (2006-2007)[105]

Sagstype		**Sager indledt af**	
Sager vedrørende miljøkriminalitet	1	Tyskland	27 %
Sager vedrørende deltagelse i en kriminel organisation	5	Nederlandene	21 %
Sager vedrørende narkotikahandel	15	Det Forenede Kongerige	15 %
Sager vedrørende skattesvig	8	Finland	13 %
Sager vedrørende svig	8	Frankrig	8 %
Sager vedrørende momssvig	1	Spanien	6 %
Sager vedrørende hvidvaskning af penge	9	Portugal	4 %
Sager vedrørende korruption	1	Sverige	2 %
Sager vedrørende formueforbrydelser	2	Danmark	2 %
Sager vedrørende våbenhandel	1	Letland	2 %
Sager vedrørende forfalskning og piratkopiering	2		
Sager vedrørende afgiftssvig	2		
Sager vedrørende forfalskning af administrative dokumenter	1		
Sager vedrørende ulovlig handel med stjålne motorkøretøjer	1		

104 "Assessing the effectiveness of EU Member States' practices in the identification, tracing, freezing and confiscation of criminal assets" – Slutrapport (for Europa-Kommissionen, GD JLS), Matrix Insight, 6.2009.

105 Ibid.

Sager vedrørende terrorisme	1
Sager vedrørende forfalskning	2
Sager vedrørende menneskehandel	1

Platforme for underretning om it-kriminalitet

Eksempler fra den franske platform for underretning om it-kriminalitet, Pharos, som har undersøgt sager om it-kriminalitet[106]	
Børnepornografi	En internetbruger underrettede Pharos om, at der fandtes en blog med fotos og tegneserielignende billeder af misbrug af børn. Bloggens redaktør, der på et billede optræder nøgen med synligt ansigt, tog også selv kontakt til børn via sin blog. Efterforskerne indkredsede en matematiklærer som hovedmistænkt. Ved en gennemsøgning af hans hjem blev der fundet 49 videoer med børnepornografi. Undersøgelsen viste også, at han havde planlagt at give hjemmeundervisning. Sagsøgte blev efterfølgende dømt og fik en betinget fængselsdom.
Misbrug af børn	Fransk politi fik et tip om, at en person tilbød penge over internettet for sex med børn. En efterforsker fra Pharos foregav at være et barn og tog kontakt med den mistænkte, som tilbød ham penge for sex. Den efterfølgende chat over internettet gjorde det muligt for Pharos at finde frem til den mistænktes IP-adresse og spore ham til en by, der er kendt for sit høje antal tilfælde af misbrug af børn. Sagsøgte blev efterfølgende dømt og fik en betinget fængselsdom.

[106] Forkortelsen Pharos står for "plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements".

Eksempler på Europols bidrag til bekæmpelse af alvorlig kriminalitet på tværs af grænserne[107]	
Operation Andromeda	I december 2009 hjalp Europol med at gennemføre en større politioperation på tværs af grænserne mod en narkoring med kontakter i 42 lande. Narkoringen havde base i Belgien og Norge og solgte narkotika fra Peru via Nederlandene til Belgien, Det Forenede Kongerige, Italien og andre medlemsstater. Politisamarbejdet blev koordineret af Europol, og det retlige samarbejde af Eurojust. De deltagende myndigheder etablerede et mobilt kontor i Pisa, og Europol et operationslokale i Haag. Europol krydsrefererede oplysninger mellem den mistænkte og udarbejdede en rapport, der gav et billede af det kriminelle netværk.
Deltagere	Italien, Nederlandene, Tyskland, Belgien, Det Forenede Kongerige, Litauen, Norge og Eurojust.
Resultater	De deltagende politistyrker beslaglagde 49 kg kokain, 10 kg heroin, 6000 ecstasypiller, to skydevåben, fem falske identitets-dokumenter og 43 000 EUR i kontanter samt arresterede 15 personer.
Operation Typhon	Mellem april 2008 og februar 2010 ydede Europol politistyrker fra 20 lande, der var involveret i operation Typhon, analytisk støtte. I denne store operation mod et pædofilt netværk, der distribuerede billeder af børnepornografi via et østrigsk websted, ydede Europol teknisk støtte og foretog strafferetlige efterretningsanalyser på grundlag af billederne fra Østrig. Det vurderede derefter dataenes pålidelighed og omstrukturerede dem, inden den udarbejdede sit eget efterretningsmateriale. Ved at krydsreferere dataene med oplysningerne i dets analysedatabase udarbejdede det 30 efterretningsrapporter, der afstedkom efterforskninger i flere lande.
Deltagere	Østrig, Belgien, Bulgarien, Canada, Danmark, Frankrig, Tyskland, Ungarn, Italien, Litauen, Luxembourg, Malta, Nederlandene, Polen, Rumænien, Slovakiet, Slovenien, Spanien, Schweiz og Det Forenede Kongerige.
Resultater	De deltagende styrker identificerede 286 mistænkte, arresterede 118 mistænkte og reddede fem ofre i fire lande, som havde været misbrugt i forbindelse med denne sag.

[107] Kommissionen modtog disse oplysninger fra Europol med henblik på denne meddelelse. Yderligere oplysninger om operation Andromeda fås på http://www.eurojust.europa.eu/.

Eurojust

Eksempler på, at Eurojust har koordineret store operationer på tværs af grænserne mellem retsmyndighederne for at bekæmpe alvorlig kriminalitet[108]	
Menneskehandel og finansiering af terrorisme	I maj 2010 koordinerede Eurojust en operation på tværs af grænserne, som førte til arrestation af fem medlemmer af et organiseret kriminelt netværk, der var aktivt i Afghanistan, Pakistan, Rumænien, Albanien og Italien. Gruppen forsynede afghanske og pakistanske statsborgere med forfalskede dokumenter og smuglede dem til Italien via Iran, Tyrkiet og Grækenland. Ved ankomsten til Italien blev migranterne sendt til Tyskland, Sverige, Belgien, Det Forenede Kongerige og Norge. Udbyttet af menneskehandlen skulle finansiere terrorisme.
Svig med bankkort	Ved at koordinere politisamarbejdet og det retlige samarbejde på tværs af grænserne hjalp Europol og Eurojust med at optrevle et netværk af bankkortsvindlere, der var aktive i Irland, Italien, Nederlandene, Belgien og Rumænien. Netværket stjal identifikationsdataene for ca. 15 000 betalingskort, hvilket medførte et tab på 6,5 mio. EUR. Forud for operationerne, der i juli 2009 førte til arrestation af 24 personer, havde belgiske, irske, italienske, nederlandske og rumænske domstole gjort det lettere at udstede europæiske arrestordre og begæringer om aflytning af de mistænkte.
Menneske- og narkotikahandel	Efter afholdelsen af et koordineringsmøde, som Eurojust organiserede i marts 2009, arresterede de italienske, nederlandske og colombianske myndigheder 62 personer, der var mistænkt for menneske- og narkotikahandel. Netværket handlede med udsatte kvinder fra Nigeria og sendte dem til Nederlandene, hvorfra de tvang dem til at prostituere sig i Italien, Frankrig og Spanien. Udbyttet af prostitutionen finansierede netværkets køb af kokain i Colombia, som blev sendt til EU med henblik på forbrug.

[108] Disse eksempler er hentet fra http://www.eurojust.europa.eu/.

PNR-oplysninger (Passenger Name Record)

Eksempler på, at en analyse af PNR-oplysninger tilvejebringer oplysninger til efterforskning af alvorlige forbrydelser på tværs af grænserne[109]	
Børnehandel	En analyse af PNR-oplysninger afslørede, at tre uledsagede børn rejste fra en EU-medlemsstat til et tredjeland, uden at det var angivet, hvem der skulle tage imod dem ved ankomsten. Efter at medlemsstatens politi efter afrejsen havde advaret tredjelandets myndigheder, arresterede de den person, der mødte op for at tage imod børnene. Det viste sig at være en seksualforbryder, der var registreret i medlemsstaten.
Menneskehandel	En analyse af PNR-oplysninger afslørede en gruppe menneske-handlere, der altid rejste ad samme rute. De brugte falske dokumenter til at checke ind på et fly inden for EU og autentiske papirer til samtidigt at checke ind på et andet fly med kurs mod et tredjeland. Når de var nået til lufthavnsloungen, gik de om bord i det fly, der fløj internt i EU.
Svig med kreditkort	Flere familier rejste til en medlemsstat på billetter, der var købt ved brug af stjålne kreditkort. Forskning viste, at en kriminel gruppe anvendte disse kort til at købe billetter, og at de solgte dem over disken i callcentre for langdistancerejser. Det var ved hjælp af PNR-oplysninger muligt at knytte de rejsende til kreditkortene og sælgerne.
Narkotikahandel	En medlemsstats politimyndigheder lå inde med oplysninger, der tydede på, at en mand var involveret i narkotikahandel i et tredjeland, men grænsevagterne fandt aldrig noget på ham, når han ankom til EU. En analyse af PNR-oplysninger viste, at han altid rejste med en associeret. En undersøgelse af hans associerede førte til, at der blev fundet store mængder narkotika.

[109] Disse eksempler er blevet anonymiseret for at beskytte kilderne til oplysningerne.

Programmet til sporing af finansiering af terrorisme (TFTP)

Eksempler på, at der ved hjælp af TFTP-oplysninger findes oplysninger til brug ved efterforskning af terrorsammensværgelser[110]	
Terrorsammen-sværgelsen i Barcelona i 2008	I januar 2008 blev ti mistænkte arresteret i Barcelona i forbindelse med et mislykket forsøg på at gennemføre et angreb på byens offentlige transportsystem. Der blev anvendt TFTP-oplysninger til at identificere de mistænktes forbindelser til Asien, Afrika og Nordamerika.
Planerne om et transatlantisk terrorangreb med flydende bomber i 2006	Der blev anvendt TFTP-oplysninger til at efterforske og dømme personer i forbindelse med et mislykket forsøg på i august 2006 at sprænge ti transatlantiske fly på vej fra Det Forenede Kongerige til USA og Canada i luften.
Bombeangrebet i London i 2005	Der blev anvendt TFTP-oplysninger til at skaffe nye spor til efterforskerne, bekræfte de mistænktes identitet og afsløre forbindelserne mellem de ansvarlige for angrebet.
Bombeangrebet i Madrid i 2004	Det blev sendt TFTP-oplysninger til flere EU-medlemsstater til brug i deres efterforskninger i kølvandet på dette angreb.

[110] Anden rapport om det amerikanske finansministeriums behandling af personoplysninger fra EU med henblik på bekæmpelse af terrorisme, dommer Jean-Louis Bruguière, januar 2010.

BILAG II

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Schengen-informations-systemet (SIS)	På initiativ af medlems-staterne.	Opretholde den offentlige orden, herunder den nationale sikkerhed i Schengenområdet og lette bevægeligheden for personer ved at benytte oplysninger, der er kommunikeret via dette system.	Centraliseret: N.SIS (nationale dele), der via en grænseflade står i forbindelse med C.SIS (centrale del).	Navn og kaldenavn, fysiske kendetegn, fødested, fødselsdato, nationalitet samt oplysninger om, hvorvidt personen er armeret eller voldelig. Indberetningerne i SIS vedrører forskellige persongrupper.	Politi, grænsepoliti, toldmyndigheder og retsmyndigheder har adgang til alle data. Indvandrings-myndighederne og de konsulære myndigheder har adgang til listen over indrejseforbud samt oplysninger om bortkomne og stjålne dokumenter. Europol og Eurojust har adgang til visse oplysninger.	Europarådets konvention 108 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Personoplysninger, der indlæses i SIS med henblik på bekæmpelse af menneskehandel, må kun lagres i det tidsrum, der er nødvendigt til det formål, hvortil de blev tilvejebragt, og højst i tre år. Oplysninger om personer, der er genstand for særlig overvågning, fordi de udgør en trussel mod den nationale sikkerhed, skal slettes efter ét år.	SIS finder fuld anvendelse i 22 medlemsstater plus Schweiz, Norge og Island. Det Forenede Kongerige og Irland deltager i SIS undtagen i forbindelse med indberetninger om tredjelandsstats-borgere på listen over indrejseforbud. Bulgarien, Rumænien og Liechtenstein forventes også snart at gennemføre det.	Signatarlandene kan foreslå ændringer af Schengen-konventionen. Den ændrede tekst skal vedtages med enstemmighed og ratificeres af parlamenterne.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Schengen-informations-system II (SIS II)	På initiativ af Kommis-sionen.	Sikre et højt beskyttelsesniveau i et område med frihed, sikkerhed og retfærdighed og lette bevægeligheden for personer ved at benytte oplysninger, der er kommunikeret via dette system.	Centraliseret: N.SIS II (nationale dele), der via en grænseflade står i forbindelse med CS.SIS (central del). SIS II vil fungere via det sikre s-TESTA-netværk.	De datakategorier, der er nævnt under SIS, plus fingeraftryk og fotos, kopier af europæiske arrestordre, indberetninger om misbrug af identitet og forbindelser mellem indberetninger. Indberetningerne i SIS II vedrører mange forskellige persongrupper.	Politi, grænsepoliti, toldmyndigheder og retsmyndigheder vil få adgang til alle data. Indvandrings-myndighederne og de konsulære myndigheder har adgang til listen over indrejseforbud samt oplysninger om bortkomne og stjålne dokumenter. Europol og Eurojust vil få adgang til visse oplysninger.	Særlige bestemmelser, der er fastsat i medfør af basisretsakterne, der regulerer SIS II, og direktiv 95/46/EF, forordning (EF) nr. 45/2001 samt Rådets rammeafgørelse 2008/977/RIA, forordning (EF) nr. 45/2001, Europarådets konvention 108 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Personoplysninger, der indlæses i SIS med henblik på at opspore personer må kun lagres i det tidsrum, der er nødvendigt til det formål, hvortil de blev tilvejebragt, og højst i tre år. Oplysninger om personer, der er genstand for særlig overvågning, fordi de udgør en trussel mod den nationale sikkerhed, skal slettes efter ét år.	SIS II er ved at blive gennemført. Når systemet er taget i drift, vil det finde anvendelse i EU-27, Schweiz, Liechtenstein, Norge og Island. Det Forenede Kongerige og Irland deltager i SIS II undtagen i forbindelse med indberetninger om tredjelandsstats-borgere på listen over indrejse-forbud.	Kommissionen skal sende halvårlige rapporter til Europa-Parlamentet og Rådet om udviklingen af SIS II og den potentielle migration fra SIS til SIS II.
Eurodac	På initiativ af Kommis-sionen.	Hjælpe med til at afgøre, hvilken medlemsstat der skal behandle en asylansøgning.	Centraliseret, består af nationale adgangspunkter, der via en grænseflade står i forbindelse med den centrale del. Eurodac fungerer via S-TESTA-netværket.	Fingeraftryksdata, køn, sted og dato for asylansøgningen, det af hjemmedlemsstaten anvendte referencenummer og den dato, hvor fingeraftrykkene blev taget, overført og indlæst i systemet.	Medlemsstaterne skal på en liste specificere, hvilke myndigheder der har adgang til dataene, hvilket typisk omfatter asyl- og migrationsmyndig-hederne, grænsevagter og politiet.	Direktiv 95/46/EF.	10 år for asylansøgeres fingeraftryk. 2 år for de tredjelandsstats-borgere, der blev pågrebet, da de på ulovlig vis passerede den ydre grænse.	Eurodac-forordningen er i kraft i alle medlemsstater, Norge, Island og Schweiz. Der er ved at blive indgået en aftale om at tilslutte Liechtenstein.	Kommissionen skal sende en årsrapport til Europa-Parlamentet og Rådet om driften af den centrale Eurodac-enhed.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Visum-informations-systemet (VIS)	På initiativ af Kommis-sionen.	Hjælpe med til at gennemføre den fælles visumpolitik og forebygge trusler mod den interne sikkerhed.	Centraliseret, består af nationale dele, der via en grænseflade står i forbindelse med den centrale del. VIS vil fungere via S-TESTA-netværket.	Visumansøgninger, fingeraftryk, fotos, tilknyttede afgørelser om visum, forbindelser mellem ansøgninger.	Visum-, asyl-, indvandrings- og grænsekontrol-myndighederne vil få adgang til alle oplysninger. Politimyndig-hederne og Europol kan søge i systemet for at forebygge, opspore og efterforske alvorlige forbrydelser.	Særlige regler fastsat i de basisretsakter, der regulerer VIS, og direktiv 95/46/EF, forordning (EF) nr. 45/2001, Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108, Europarådets tillægsprotokol 181 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	5 år.	VIS er ved at blive gennemført og vil blive anvendt i alle medlemsstater (med undtagelse af Det Forenede Kongerige og Irland) plus Norge, Island og Schweiz.	Kommissionen skal rapportere til Europa-Parlamentet og Rådet om driften af VIS tre år efter, at systemet er taget i drift, og derefter hvert fjerde år.
API-oplysninger (Advanced Passenger Information)	På initiativ af Spanien.	Forbedre grænsekontrollen og bekæmpe ulovlig indvandring.	Decentraliseret.	Personoplysninger fra pas, påstigningssted, indrejsested i EU.	Grænsekontrol-myndighederne og på anmodning de retshåndhævende myndigheder.	Direktiv 95/46/EF.	Oplysningerne skal slettes 24 timer efter flyets ankomst til EU.	API er kraft i alle medlemsstater, men kun nogle få af dem bruger det.	Kommissionen vil evaluere API-systemet i 2011.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Napoli II-konven-tionen	På initiativ af medlems-staterne.	Bistå de nationale toldmyndigheder med at forebygge og opspore overtrædelser af de nationale toldbestemmelser og bistå dem med at retsforfølge og straffe overtrædelser af EU-toldbestemmelser og nationale toldbestemmelser.	Decentraliseret, fungerer via et sæt centrale koordinerings-enheder	Alle oplysninger vedrørende en identificeret eller identificerbar statsborger.	De centrale koordinerings-enheder sender oplysninger til de nationale toldmyndigheder, efterforsknings-myndighederne og, forudsat at den medlemsstat, der har sendt oplysningerne, giver sit forudgående tilsagn hertil, til andre myndigheder.	Direktiv 95/46/EF og Europarådets konvention 108. Oplysningerne skal i den modtagende medlemsstat være omfattet af et beskyttelsesniveau, der mindst svarer til det, der findes i den sendende medlemsstat.	De videregivne oplysninger må ikke lagres længere end, hvad der er nødvendigt til det formål, hvortil de blev videregivet.	Alle medlemsstater har ratificeret denne konvention.	Signatarlandene kan foreslå ændringer af Napoli II-konventionen. Den ændrede tekst skal vedtages af Rådet og ratificeres af medlemsstaterne.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Toldinformations-systemet (CIS)	På initiativ af medlems-staterne.	Bistå de kompetente myndigheder med at forebygge, efterforske og retsforfølge alvorlige overtrædelser af den nationale toldlovgivning.	Centraliseret, adgang hertil via terminaler i hver medlemsstat og i Kommissionen. CIS og FIDE fungerer på grundlag af AFIS, der anvender CCN-netværket (Common Communication Network), CIS-netværket (Common System Interface) eller Kommissionens sikre webadgang.	Navn og kaldenavn, fødested, fødselsdato, nationalitet, køn, fysiske kendetegn, identifikations-dokumenter, adresse, forudgående tilfælde af vold, årsager til at medtage oplysningerne i CIS, forslag til, hvad der skal gøres, samt registrering af transportmidler.	Nationale toldmyndigheder, Europol og Eurojust har adgang til CIS-data.	Særlige regler i CIS-konventionen og direktiv 95/46/EF, forordning (EF) nr. 45/2001, Europarådets konvention 108 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Personoplysninger kopieret fra CIS til andre systemer med henblik på risikoforvaltning eller operationelle analyser må kun opbevares i det tidsrum, der er nødvendigt til det formål, hvortil de blev kopieret, og højst i 10 år.	I kraft i alle medlemsstater.	Kommissionen rapporterer i samarbejde med medlemsstaterne hvert år til Europa-Parlamentet og Rådet om driften af CIS.
Svensk initiativ	På initiativ af Sverige.	Strømline udvekslingen af oplysninger med henblik på strafferetlig efterforskning og strafferetlig efterretning.	Decentraliseret, medlemsstaterne skal udpege nationale kontaktpunkter, der tager sig af hastende anmodninger om oplysninger.	Alle eksisterende oplysninger eller strafferetlige efterretninger, som de retshåndhævende myndigheder har til rådighed.	Politi, toldmyndigheder og alle andre myndigheder med kompetence til at efterforske forbrydelser (med undtagelse af efterretnings-tjenesterne).	Nationale databeskyttelses-regler samt Europarådets konvention 108, Europarådets tillægsprotokol 181 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Oplysninger og efterretninger, der tilvejebringes ved hjælp af dette instrument, kan kun bruges til det formål, hvortil de blev tilvejebragt, og på særlige betingelser, som den sendende medlemsstat har fastsat.	12 ud af 31 signatarlande (EU- og EFTA-stater) har vedtaget national lovgivning om gennemførelse af dette instrument. Fem af dem udfylder formularen til anmodning om oplysninger, og to bruger det hyppigt til informations-udveksling.	Kommissionen skal forelægge sin evalueringsrapport for Rådet i 2010.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Prümafgø-relsen	På initiativ af medlems-staterne.	Forbedre forebyggelsen af forbrydelser, navnlig terrorisme, og opretholde den offentlige orden.	Decentraliseret, indbyrdes forbundet via S-TESTA-netværket. De nationale kontaktpunkter tager sig af udgående og indkommende anmodninger om datasammen-ligning.	Anonyme dna-profiler og fingeraftryk, registreringsdata for motorkøretøjer og oplysninger om enkeltpersoner, der er mistænkt for at have forbindelse til terrorisme.	Kontaktpunkter sender anmodninger. Hvem, der har adgang på nationalt plan, er fastsat i national lovgivning.	Særlige regler fastsat ved Prümafgørelsen og Europarådets konvention 108, Europarådets tillægsprotokol 181 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger. Enkeltpersoner kan rette henvendelse til deres nationale databeskyttelses-tilsynsmyndig-heder for at håndhæve deres rettigheder, hvad angår behandling af personoplysninger.	Personoplysninger skal slettes, når de ikke længere er nødvendige til det formål, hvortil de blev tilvejebragt. Den maksimale længde af den nationale datalagringsperiode i den sendende stat er bindende for den modtagende stat.	Prümafgørelsen er ved at blive gennemført. 10 medlemsstater har fået bemyndigelse til at udveksle dna-oplysninger, 5 til at udveksle fingeraftryks-oplysninger og 7 til at udveksle oplysninger fra motorkøretøjs-registre. Norge og Island er ved at tilslutte sig.	Kommissionen skal forelægge sin evalueringsrapport for Rådet i 2012.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Datalag-ringsdirek-tivet	På initiativ af medlems-staterne.	Forbedre efterforskningen, opsporingen og retsforfølgningen af alvorlige forbrydelser ved at lagre oplysninger om datatrafik og lokaliserings-oplysninger i forbindelse med telekommuni-kation.	Decentraliseret, dette instrument pålægger udbyderne af telekommunika-tionstjenester at lagre data.	Telefonnummer, IP-adresse, mobiltelefon-apparaters identifikatorer.	Hvilke myndigheder, der har adgangsret, fastsættes på nationalt plan.	Direktiv 95/46/EF og direktiv 2002/58/EF.	Fra 6 til 24 måneder.	Seks medlemsstater har endnu ikke gennemført datalagrings-direktivet i national lovgivning, og den tyske og den rumænske forfatningsret har fastslået, at gennemførelses-bestemmelserne er i strid med forfatningen.	Kommissionen skal forelægge sin evalueringsrapport for Europa-Parlamentet og Rådet i 2010.
Det europæiske informa-tionssystem vedrørende straffe-registre (ECRIS)	På initiativ af Belgien og efter forslag af Kommis-sionen.	Forbedre udvekslingen af oplysninger på tværs af grænserne vedrørende EU-borgeres straffeattester.	Decentraliseret, indbyrdes forbundet via et sæt centrale myndigheder, der via s-TESTA-netværket vil udveksle oplysninger fra strafferegistre.	Personlige oplysninger, domme og lovovertrædelser, supplerende oplysninger, herunder fingeraftryk (hvis de foreligger).	Retsmyndig-hederne og de kompetente administrative myndigheder.	Særlige regler fastsat i Rådets rammeafgørelse 2009/315/RIA, som omfatter reglerne i Rådets afgørelse 2005/876/RIA og Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108 og forordning (EF) nr. 45/2001.	Nationale datalagringsregler finder anvendelse, da dette instrument kun regulerer udvekslingen af oplysninger.	ECRIS er ved at blive gennemført. 9 medlemsstater har påbegyndt den elektroniske udveksling af oplysninger.	Kommissionen skal forelægge to evalueringsrapporter for Europa-Parlamentet og Rådet: vedrørende rammeafgørelse 2008/675/RIA i 2011 og vedrørende rammeafgørelse 2009/315/RIA i 2015. Fra 2016 skal Kommissionen regelmæssigt offentliggøre rapporter om, hvordan rammeafgørelse 2009/316/RIA fungerer.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Samarbejde inden for rammerne af den finansielle efterret-ningsenhed (FIU.net)	På initiativ af Neder-landene.	Udveksle de oplysninger, der er nødvendige for at analysere og efterforske hvidvaskning af penge og finansiering af terrorisme.	Decentraliseret, FIU's udveksling af oplysninger via FIU.net, der fungerer på s-TESTA-netværket. Europols Siena-applikation kan snart understøtte FIU.net.	Alle oplysninger af relevans for analysen eller efterforskningen af hvidvaskning af penge og finansiering af terrorisme.	Den finansielle efterretningsenhed (inden for politistyrken, retsmyndighederne eller de administrative myndigheder, der rapporterer til de finansielle myndigheder).	Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Nationale datalagringsregler finder anvendelse, da dette instrument kun regulerer udvekslingen af oplysninger.	20 medlemsstater deltager i FIU.net, en onlinedata-udvekslings-applikation, der fungerer via s-TESTA.	Kommissionen har som en del af sin handlingsplan for finansielle tjenesteydelser siden 2009 evalueret gennemførelsen af direktiv 2005/60/EF.
ARO-samarbej-det (samarbej-det mellem medlems-staternes kontorer for inddrivelse af aktiver (ARO)	På initiativ af medlems-staterne.	Udveksle de oplysninger, der er nødvendige for at spore og identificere udbyttet af kriminalitet.	Decentraliseret, ARO-kontorerne skal via det svenske initiativ udveksle oplysninger. Europols Siena-applikation kan snart understøtte ARO-samarbejdet.	Nærmere detaljer om de pågældende formuegoder såsom bankkonti, fast ejendom og motorkøretøjer samt nærmere oplysninger om personer såsom navn, adresse, aktionær og virksomheds-oplysninger.	Kontorer for inddrivelse af aktiver.	Europarådets konvention 108, Europarådets tillægsprotokol 181, Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Nationale datalagringsregler finder anvendelse, da dette instrument kun regulerer udvekslingen af oplysninger.	Flere end 20 medlemsstater har etableret kontorer til inddrivelse af aktiver; 12 deltager i et pilotprojekt, hvor Europols Siena-applikation blev anvendt til at udveksle oplysninger, der er relevante for at opspore aktiver.	Kommissionen skal forelægge sin evalueringsrapport for Rådet i 2010.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
It-kriminalitetsplatforme på nationalt plan og EU-plan	På initiativ af Frankrig.	Indsamle, udveksle og analysere oplysninger om lovovertrædelser begået på internettet.	Decentraliseret, samle nationale indberetnings-platforme og Europols it-kriminalitets-platform i EU. Europols Siena-applikation kan snart understøtte dataudvekslingen mellem indberetnings-platforme.	Ulovligt indhold eller adfærd, der opspores på internettet.	Nationale platforme modtager indberetninger fra borgere. Europols it-kriminalitets-platform i EU modtager rapporter fra retshåndhævende myndigheder vedrørende alvorlig it-kriminalitet på tværs af grænserne.	Særlige regler fastsat i Europol-afgørelsen og Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108, Europarådets tillægsprotokol 181 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Nationale datalagringsregler finder anvendelse, da denne foranstaltning kun regulerer udvekslingen af oplysninger.	Næsten alle medlemsstater har etableret nationale platforme for indberetning. Europol arbejder på sin it-kriminalitets-platform i EU.	Europol dækker it-kriminalitet og vil fremover rapportere om aktiviteterne i it-kriminalitets-platformen i EU i sin årsrapport, der indgives til Rådet, der skal godkende den, og til Europa-Parlamentet til orientering.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Europol	På initiativ af medlems-staterne.	Støtte medlemsstaterne i deres bestræbelser for at forebygge og bekæmpe organiseret kriminalitet, terrorisme og andre alvorlige forbrydelser, der vedrører to eller flere medlemsstater.	Europol er et EU-agentur med sæde i Haag. Det udvikler Siena, dets eget sikre netværksapplika-tion for sikker informations-udveksling.	Europols informationssystem (EIS) indeholder personoplysninger, herunder biometriske identifikatorer, domme og oplysninger om forbindelse til organiseret kriminalitet, for personer, der mistænkes for kriminalitet, som falder ind under Europols mandat. Analysedatabasen indeholder personoplysninger af relevans.	Europols nationale enheder, forbindelses-officerer, personale og direktør har adgang til EIS. Forbindelses-officerer har adgang til analysedatabasen. Personoplysninger kan udveksles med tredjelande, der har aftaler med Europol.	Særlige regler fastsat i Europol-afgørelsen og Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108, Europarådets tillægsprotokol 181 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Filer i analysedatabane kan højst lagres i 3 år, med mulighed for at forlænge det tidsrum med yderligere 3 år.	Europol bruges aktivt af alle medlemsstater og tredjelande, som det har indgået operationelle aftaler med. Europols nye retsgrundlag er blevet gennemført af alle medlemsstater.	Et fælles tilsynsorgan overvåger Europols behandling af personoplysninger og overførslen af disse til andre parter. Det indgiver regelmæssigt rapport til Europa-Parlamentet og Rådet. Europol indgiver også en årsrapport om sine aktiviteter til Rådet, der skal godkende den, og til Europa-Parlamentet til orientering.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
Eurojust	På initiativ af medlems-staterne.	Forbedre koordineringen af efterforskning og retsforfølgning i medlemsstaterne og øge samarbejdet mellem de relevante myndigheder.	EU-organ med sæde i Haag. Det anvender s-TESTA til dataudveksling.	Personoplysninger for mistænkte og lovovertrædere i sager vedrørende alvorlig kriminalitet, der berører to eller flere medlemsstater, herunder personlige oplysninger, kontaktoplysninger, dna-profiler, fingeraftryk, fotos og datatrafik og lokaliserings-oplysninger i forbindelse med telekommunikation.	Europols 27 nationale medlemmer, der kan udveksle data med nationale myndigheder og tredjelande, hvis kilden til de originale oplysninger er indforstået hermed.	Særlige regler fastsat i den retsakt, der regulerer Eurojust og Rådets rammeafgørelse 2008/977/RIA, Europarådets konvention 108, Europarådets tillægsprotokol 181 og Europarådets henstilling R (87) 15 om politiets brug af personoplysninger.	Oplysningerne skal slettes, når de har tjent det formål, hvortil de blev tilvejebragt, og når sagen er afsluttet.	Medlemsstaterne er ved at gennemføre det ændrede retsgrundlag for Eurojust.	Inden juni 2014 skal Kommissionen evaluere dataudvekslingen mellem Eurojusts nationale medlemmer. Inden juni 2013 skal Eurojust rapportere til Rådet og Kommissionen om adgang til dets sagsforvaltnings-system. Et fælles tilsynsorgan overvåger Eurojusts behandling af personoplysninger og rapporterer hvert år til Rådet. Formanden for Eurojust-kollegiet indgiver en årsrapport til Rådet om Eurojusts aktiviteter, som Rådet videresender til Europa-Parlamentet.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
PNR-aftaler med USA, og Australien; API/PNR-aftale med Canada	På initiativ af Kommis-sionen.	Forebygge og bekæmpe terrorisme og andre former for alvorlig tværnational kriminalitet.	Internationale aftaler.	Aftalerne med USA og Australien indeholder 19 PNR-datakategorier, herunder personlige oplysninger, reservations- og betalingsoplysninger samt supplerende oplysninger. Den canadiske aftale indeholder 25 lignende dataelementer.	USA's ministerium for national sikkerhed, Canadas grænsemyndig-heder og Australiens toldmyndigheder, som kan dele oplysninger med retshåndhævende myndigheder og antiterrortjenester.	Der fastsættes databeskyttelses-regler i disse særlige internationale aftaler.	USA: aktiv brug i 7 år og passiv brug i 8 år; Australien: aktiv brug i 3,5 år og passiv brug i 2 år; Canada: aktiv brug i 72 timer og passiv brug i 3,5 år.	Aftalerne med USA og Australien finder midlertidigt anvendelse; den canadiske aftale er trådt i kraft. Kommissionen vil genforhandle disse aftaler. I EU har seks medlemsstater vedtaget lovgivning, der gør det muligt at anvende PNR-oplysninger med henblik på retshåndhævelse.	Hver aftale indeholder bestemmelser om regelmæssig evaluering, og den canadiske og den australske aftale indeholder desuden bestemmelser om aftalens ophør.

Overblik i tabelform over instrumenter, der anvendes, er ved at blive gennemført eller overvejes

Instrument	Baggrund	Formål	Struktur	Type personoplysninger	Hvem har adgang til oplysningerne	Databeskyttelse	Lagring af oplysninger	Gennemførelses-fase	Evaluering
TFTP-aftale mellem EU og USA	På initiativ af Kommis-sionen.	Forebygge, efterforske, opspore eller retsforfølge terrorisme eller finansiering af terrorisme.	International aftale.	Finansielle betalingsdata, der bl.a. indeholder navn på, kontonummer for, adresse på og id-nummer for dem, der står bag finansielle transaktioner og modtagerne heraf.	Det amerikanske finansministerium kan med henblik på TFTP-programmet udveksle personoplysninger, der er udtrukket af finansielle betalingsdata med de amerikanske retshåndhævende myndigheder, myndigheder med ansvar for den offentlige orden eller antiterrormyndig-heder, medlemsstaterne, Europol eller Eurojust. Videregivelse til tredjelande må kun ske med medlemsstaternes samtykke.	Aftalen indeholder strenge bestemmelser om formålsbegræns-ning og forholdsmæssig-hed.	Personoplysninger, der er udtrukket af finansielle betalingsdata, må ikke lagres længere end, hvad der er nødvendigt med henblik på individuelle efterforskninger eller retsforfølgninger. Ikke-udtrukne oplysninger må kun lagres i 5 år.	Europa-Parlamentet godkendte indgåelsen af TFTP-aftalen mellem EU og USA den 20. juli 2010. Rådet forventes nu at vedtage Rådets afgørelse om indgåelse af aftalen, hvorefter aftalen træder i kraft via brevveksling mellem parterne.	Kommissionen skal evaluere denne aftale seks måneder efter, at den er trådt i kraft. Evalueringsrapporten skal sendes til Europa-Parlamentet og Rådet.