EUROPEISKA KOMMISSIONEN

Bryssel den 20.7.2010

KOM(2010)385 slutlig

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa

1. INLEDNING

Europeiska unionen har kommit långt sedan ledarna för fem europeiska länder 1985 i Schengen enades om att avskaffa kontrollerna vid de berörda ländernas gemensamma gränser. Avtalet ledde 1990 till Schengenkonventionen, som innehöll fröet till många av dagens strategier för informationshantering. Avskaffandet av kontrollerna vid de inre gränserna har sporrat utvecklingen av en hel rad åtgärder vid de yttre gränserna, huvudsakligen avseende viseringar, samordning av asyl- och invandringspolitiken samt en förstärkning av polissamarbetet, det rättsliga samarbetet och tullsamarbetet i kampen mot gränsöverskridande brottslighet. Varken Schengenområdet eller den inre marknaden skulle fungera idag utan ett gränsöverskridande informationsutbyte.

Terrorattackerna i Förenta staterna 2001 samt bombningarna i Madrid och London 2004 respektive 2005 utlöste en ny dynamik i utvecklingen av EU:s politik för informationshantering. Under 2006 antog rådet och Europaparlamentet direktivet om lagring av uppgifter, i syfte att göra det möjligt för nationella myndigheter att bekämpa allvarlig brottslighet genom att lagra telefontrafik- och lokaliseringsuppgifter.[1] Rådet tog därefter fasta på det svenska initiativet om att underlätta utbytet av information mellan medlemsstaterna i samband med brottsutredningar och underrättelseverksamhet. År 2008 godkände man det så kallade Prümbeslutet om att snabba på utbytet av DNA-profiler, fingeravtryck och uppgifter ur fordonsregister i kampen mot terrorism och andra former av brottslighet. Gränsöverskridande samarbete mellan finansunderrättelseenheter, nationella kontor för återvinning av tillgångar, plattformar för bekämpning av IT-brottslighet samt medlemsstaternas användning av Europol och Eurojust är andra verktyg i kampen mot allvarlig brottslighet i Schengenområdet.

Mycket snart efter terrorattackerna den 11 september 2001 inrättade Förenta staternas regering ett program för att spåra finansiering av terrorism. Syftet var att genom övervakning av misstänkta ekonomiska transaktioner förhindra att liknande planer sätts i verket. Europaparlamentet har nyligen gett sitt samtycke till ingåendet av avtalet mellan EU och Förenta staterna om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från EU till Förenta staterna som ett led i programmet för att spåra

[1] Det finns för närvarande ingen harmoniserad EU-definition av ”allvarlig brottslighet”. I det rådsbeslut varigenom Europol bemyndigas att göra sökningar i VIS (rådets beslut 2008/633/RIF, EUT L 218, 13.8.2008, s. 129) definieras ”allvarliga brott” genom en hänvisning till förteckningen över brott i den europeiska arresteringsordern (rådets beslut 2002/584/RIF, EGT L 190, 18.7.2002, s. 1). Direktivet om lagring av uppgifter (direktiv 2002/58/EG, EUT L 105, 13.4.2006, s. 54) överlämnar åt medlemsstaterna att definiera vad som utgör ett ”allvarligt brott”. Europolbeslutet (rådets beslut 2009/371/RIF, EUT L 121, 15.5.2009, s. 37) innehåller en annan förteckning över brott som definieras som ”allvarliga”. Denna förteckning är mycket lik, om än inte identisk med förteckningen i den europeiska arresteringsordern.

finansiering av terrorism (TFTP-avtalet mellan EU och Förenta staterna).[2] Utbytet mellan EU och tredjeländer av passageraruppgifter (PNR) och förhandsupplysningar om passagerare har också bidragit till EU:s kapacitet att bekämpa terrorism och annan allvarlig brottslighet.[3] Efter att ha ingått PNR-avtal med Förenta staterna, Australien och Kanada, har kommissionen nyligen återvänt till ritbordet för att se över sin strategi när det gäller att inrätta ett PNR-system i EU och dela med sig av dessa uppgifter till tredjeländer.

Ovannämnda åtgärder har skapat förutsättningar för fri rörlighet i Schengenområdet, bidragit till att förebygga och bekämpa terrorattacker och andra former av allvarlig brottslighet samt stärkt utvecklingen av en gemensam viserings- och asylpolitik.

Genom detta meddelande ges för första gången en full överblick över åtgärder på EU-nivå som redan har införts, som håller på att genomföras eller är under övervägande när det gäller insamling, lagring eller gränsöverskridande utbyte av personuppgifter för ändamål som rör brottsbekämpning eller migrationshantering. Människor i EU har rätt att veta vilka personuppgifter som utbyts om dem, vem som genomför detta utbyte och ändamålen med utbytet. Detta dokument besvarar dessa frågor på ett öppet sätt och förklarar huvudsyftet med instrumenten, hur instrumenten är uppbyggda och vilka typer av uppgifter som omfattas. Vidare tar meddelandet upp vilka myndigheter som har tillgång till uppgifterna i fråga samt gällande bestämmelser om skydd och lagring av uppgifter. Det innehåller också ett antal exempel som beskriver hur dessa instrument fungerar i praktiken (se bilaga I). Slutligen anges de viktigaste av de principer som bör ligga till grund för utformningen och utvärderingen av informationshanteringen inom området med frihet, säkerhet och rättvisa.

Genom att ge en överblick över de åtgärder på EU-nivå som reglerar hanteringen av personuppgifter och framhålla en uppsättning principer för utarbetandet och bedömningen av sådana åtgärder, bidrar detta meddelande till en väl underbyggd dialog om strategier med alla berörda parter. Samtidigt kan meddelandet ses som ett första svar på medlemsstaternas önskan om att utveckla en mer samlad strategi för utbytet av personuppgifter för brottsbekämpningsändamål, en fråga som nyligen togs upp i EU-strategin för informationshantering,[4] och som ett underlag för eftertanke kring ett eventuellt behov av att utveckla en europeisk modell för informationsutbyte på grundval av en utvärdering av befintliga åtgärder på området.[5]

Ändamålbegränsning är en mycket viktigt inslag i de flesta av de instrument som omfattas av meddelandet. Ett enda övergripande informationssystem som fyller flera funktioner skulle ge det effektivaste informationsutbytet. Att skapa ett sådant system skulle dock innebära en grov och orättmätig begränsning av individens rätt till integritet och skydd för sina personuppgifter och skapa enorma problem när det gäller utveckling och drift. I praktiken har politiken inom området med frihet, säkerhet och rättvisa utvecklats stegvis, vilket har lett till en rad informationssystem och instrument av olika omfattning och med varierande räckvidd och

---

2 Europaparlamentets resolution, P7 TA-PROV (2010)0279, 8.7.2010.

3 I motsats till ”allvarligt brott” definieras ”terroristbrott” mycket klart i rådets rambeslut om bekämpande av terrorism (rådets rambeslut 2002/475/RIF, EGT L 164, 22.6.2002, s. 3, ändrat genom rådets rambeslut 2008/919/RIF, EUT L 330, 9.12.2008, s. 21).

4 Rådets slutsatser om en informationshanteringsstrategi för EU:s inre säkerhet, rådet (rättsliga och inrikes frågor), 30.11.2009 (EU:s informationshanteringsstrategi), frihet, säkerhet, personlig integritet — europeiska inrikes frågor i en öppen värld, rapport från den informella rådgivande högnivågruppen avseende framtiden för den europeiska politiken för inrikes frågor (framtidsgruppen), juni 2008.

5 Stockholmsprogrammet — ett öppet och säkert europa i medborgarnas tjänst och för deras skydd, rådets dokument 5731/10, 3.3.2010, avsnitt 4.2.2.

syfte. Den uppdelade informationshanteringsstruktur som har växt fram de senaste decennierna är mer lämpad att skydda medborgarnas rätt till integritet än något centraliserat alternativ.

Detta meddelande omfattar inte åtgärder som rör utbyte av uppgifter som inte är personuppgifter för strategiska ändamål, till exempel allmänna riskanalyser eller hotbedömningar. Det ger inte heller någon detaljerad analys av bestämmelserna om uppgiftsskydd i de instrument som är under diskussion, eftersom kommissionen för närvarande är i färd med att göra en särskild utvärdering av möjligheterna att införa en ny övergripande ram för skyddet av personuppgifter i EU. Rådet överväger för närvarande utkastet till förhandlingsdirektiv för ett avtal mellan EU och Förenta staterna om uppgiftsskydd vid överföring och behandling av uppgifter i syfte att förebygga, utreda, upptäcka och lagföra brott, inklusive terrorism, inom ramen för polissamarbetet och det straffrättsliga samarbetet. Eftersom dessa förhandlingar förväntas fastställa vilka sätt de två parterna kan använda sig av för att garantera en starkt skydd för de grundläggande fri- och rättigheterna vid överföring av personuppgifter, snarare än själva innehållet i sådan överföring behandling av uppgifter, omfattas det initiativet inte av det här meddelandet.[6]

2. EU-INSTRUMENT OM INSAMLING, LAGRING OCH UTBYTE AV PERSONUPPGIFTER FÖR BROTTSBEKÄMPNINGS- ELLER MIGRATIONSHANTERINGSÄNDAMÅL

I detta avsnitt görs en genomgång av Europeiska unionens rättsakter om insamling, lagring och gränsöverskridande utbyte av personuppgifter för brottsbekämpnings- och migrationshanteringsändamål. Avsnitt 2.1 sätter fokus på bestämmelser som gäller för närvarande, håller på att genomföras eller är under övervägande, medan avsnitt 2.2 rör initiativ som tas upp i handlingsplanen för att genomföra Stockholmsprogrammet.[7] Genomgången ger information om följande aspekter av respektive instrument:

– Bakgrund (huruvida åtgärden föreslogs av medlemsstater eller kommissionen)[8].

– Ändamålet med insamlingen, lagringen eller utbytet av uppgifter.

– Struktur (centraliserade informationssystem eller decentraliserat utbyte av uppgifter).

– Personuppgifter som omfattas.

– Myndigheter med tillgång till uppgifterna.

– Bestämmelser om uppgiftsskydd.

– Bestämmelser om lagring av uppgifter.

---

6 KOM(2010) 252, 26.5.2010.

7 KOM(2010) 171, 20.4.2010 (handlingsplanen för genomförandet av Stockholmsprogrammet).

8 I Europeiska unionens tidigare tredje pelare, som omfattade polissamarbetet och det straffrättsliga samarbetet, hade medlemsstaterna och kommissionen delad initiativrätt. Genom Amsterdamfördraget införlivades områdena yttre gränskontroll, viseringar, asyl och invandring med gemenskapens första pelare, där kommissionen hade exklusiv initiativrätt. Genom Lissabonfördraget avskaffades unionens pelarstruktur, och kommissionens initiativrätt bekräftades. När det gäller polissamarbetet och det straffrättsliga samarbetet (inklusive administrativt samarbete) kan lagstiftning emellertid fortfarande föreslås på initiativ av en fjärdedel av medlemsstaterna.

– Genomförandeläge.

– Översynsmekanism.

2.1. Gällande instrument samt instrument under genomförande eller övervägande

EU-instrument som syftar till att förbättra samarbetet inom Schengenområdet

Schengens informationssystem (SIS) växte fram ur medlemsstaternas önskan att skapa ett område utan kontroller vid de inre gränserna och samtidigt underlätta för människor att förflytta sig över deras yttre gränser.[9] Systemet, som varit i drift sedan 1995, syftar till att upprätthålla den allmänna säkerheten, inbegripet den nationella säkerheten, inom Schengenområdet. SIS är ett centraliserat informationssystem som består av en nationell del i var och en av de deltagande staterna och en teknisk stödfunktion i Frankrike. Medlemsstaterna kan registrera personer som har efterlysts för förvarstagande för utlämning, tredjelandsmedborgare som ska vägras inresa, saknade personer, vittnen eller andra som är kallade till rättegång, personer eller fordon som är föremål för särskild övervakning på grund av det hot de utgör för den allmänna eller den nationella säkerheten, försvunna eller stulna motorfordon, handlingar och skjutvapen samt misstänkta sedlar. Till de uppgifter som läggs in i SIS hör namn och antagna namn, fysiska kännemärken, födelsedatum och födelseort, medborgarskap och huruvida en person är beväpnad och våldsbenägen. Polis, gränskontroll, tull och rättsliga myndigheter som handlägger straffrättsliga förfaranden har tillgång till uppgifterna i enlighet med sina respektive lagstadgade befogenheter. Invandringsmyndigheter och konsulat har tillgång till uppgifter om tredjelandsmedborgare som ska vägras inresa samt registreringar om försvunna eller stulna handlingar. Europol kan få tillgång till vissa kategorier av uppgifter i SIS, inklusive uppgifter om personer som har efterlysts för förvarstagande för utlämning och uppgifter om personer som är föremål för särskild övervakning på grund av det hot de utgör för den allmänna eller den nationella säkerheten. Eurojust kan få tillgång till uppgifter om personer som har efterlysts för förvarstagande för utlämning samt uppgifter om vittnen eller personer som inte har följt en kallelse att inställa sig vid domstol. Personuppgifter får endast användas för de särskilda typer av registreringar för vilka de lämnats ut. Personuppgifter som förts in i SIS i syfte att spåra personer får endast lagras så länge som är motiverat med hänsyn till syftet med registreringen, dock aldrig längre än tre år från det att uppgifterna infördes. Uppgifter om personer som är föremål för särskild övervakning på grund av det hot de utgör för den allmänna eller den nationella säkerheten ska raderas inom ett år. Medlemsstaterna ska införa nationella bestämmelser som ger en skyddsnivå för personuppgifter som åtminstone motsvarar den som följer av principerna i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter och är förenlig med Europarådets ministerkommittés rekommendation R (87) 15 av den 17 september 1987 avseende reglering av användningen av personuppgifter inom den polisiära sektorn (nedan kallad *polisrekommendationen*).[10] Schengenkonventionen innehåller ingen översynsmekanism, vilket innebär att det är det är de undertecknande staterna som ska föreslå eventuella ändringar. Om så sker måste den ändrade

---

[9] Konvention om tillämpning av Schengenavtalet av den 14 juni 1985 mellan regeringarna i Beneluxstaterna, Förbundsrepubliken Tyskland och Franska republiken om gradvis avskaffande av kontroller vid de gemensamma gränserna, EGT L 239, 22.9.2000, s. 19.

[10] Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 28.1.1981 (Europarådets konvention nr 108), Europarådets ministerkommittés relommendation nr R (87) 15 avseende reglering av användningen av personuppgifter inom den polisiära sektorn, Europarådet, 17.9.1987 (polisrekommendationen).

texten antas genom enhälligt beslut och ratifceras av de nationella parlamenten. SIS tillämpas fullt ut i 22 medlemsstater samt i Schweiz, Norge och Island. Förenade kungariket och Irland. Förenade kungariket och Irland deltar i de delar av Schengen och SIS som rör polissamarbete, med undantag för uppgifter om tredjelandsmedborgare som ska vägras inresa. Cypern har undertecknat Schengenkonventionen, men ännu inte genomfört den. Liechtenstein kommer att genomföra den 2010 och Bulgarien och Rumänien förväntas genomföra den 2011. Sökningar i SIS resulterar i en ”träff” när uppgifterna om en person eller ett föremål matchar uppgifterna i en befintlig registrering. Brottsbekämpande myndigheter som får en träff kan, via sitt nätverk av Sirenekontor, begära ytterligare information om föremålet för en registrering.[11]

I och med att nya medlemsstater har anslutit sig till Schengensamarbetet har SIS-databasen vuxit i motsvarande omfattning: mellan januari 2008 och januari 2010 steg antalet SIS-registreringar från 22,9 till 31,6 miljoner.[12] Medlemsstaterna, som förutsåg denna ökning av datavolymerna och förändringar av användarnas behov, beslutade 2001 att utveckla en **andra generation av Schengens informationssystem** (SIS II). Uppgiften att genomföra detta anförtroddes åt kommissionen.[13] Syftet med SIS II, som för närvarande är under utveckling, är att säkerställa en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa genom att få funktionerna i den första generationens system att fungera bättre och att underlätta rörligheten för personer som använder uppgifter som meddelas via detta system. Dessutom kommer SIS II, utöver de ursprungliga uppgiftskategorier som omfattas den första generationens system, även att kunna hantera fingeravtryck, fotografier, kopior av den europeiska arresteringsordern, bestämmelser för att skydda personer vars identitet missbrukas och länkar mellan olika registreringar. SIS II kommer till exempel att kunna länka samman registreringarna rörande en person som är efterlyst för bortförande, rörande den person som bortförts respektive rörande det fordon som använts vid brottet. Åtkomsträttigheterna och bestämmelserna om lagring av uppgifter är identiska med dem i första generationens system. Personuppgifter får endast användas med avseende på de särskilda registreringar för vilka de tillhandahållits. Personuppgifter i SIS II ska behandlas i enlighet med de särskilda bestämmelserna i de rättsakter som ligger till grund för systemet (förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF), som klargör principerna i direktiv 95/46/EG, och i enlighet med förordning (EG) nr 45/2001, Europarådets konvention nr 108 och polisrekommendationen.[14] SIS II kommer att använda s-Testa, kommissionens säkra nätverk för datakommunikation.[15] När detta system tagits i drift kommer det att användas i EU:s 27 medlemsstater samt i Schwiez, Liechtenstein, Norge och Island.[16] Kommissionen ska

---

11 Sirenestandarder för framställningar om ytterligare information vid sökningar av nationella myndigheter.

12 Rådets dok. 5441/08, 30.1.2008, rådets dok. 6162/10, 5.2.2010.

13 Förordning (EG) nr 1986/2006, EUT L 381, 28.12.2006, s. 1; förordning (EG) nr 1987/2006, EUT L 381, 28.12.2006, s. 4; beslut 2007/533/RIF, EUT L 205, 7.8.2007, p. 63.

14 Förordning (EG) nr 1987/2006, EUT L 381, 28.12.2006, s. 4; beslut 2007/533/RIF, EUT L 205, 7.8.2007, s. 63; direktiv 95/46/EG, EGT L 281, 23.11.1995, s. 31; förordning (EG) nr 45/2001, EGT L 8, 12.1.2001, s. 1; konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 28.1.1981 (Europarådets konvention nr 108); Europarådets ministerkommittés relommendation nr R (87) 15 avseende reglering av användningen av personuppgifter inom den polisiära sektorn, Europarådet, 17.9.1987 (polisrekommendationen).

15 S-Testa, som står för *Secure Trans-European Services for Telematics between Administrations*, är ett kommissionsfinansierat nätverk för datakommunikation som möjliggör ett säkert och krypterat utbyte av upplysningar mellan nationella förvaltningar och EU:s institutioner, byråer och organ.

16 Förenade kungariket och Irland kommer att delta i SIS II, med undantag för den del som rör registreringar av tredjelandsmedborgare som finns upptagna på förteckningen över personer med inreseförbud.

varannat år överlämna en lägesrapport till Europaparlamentet och rådet om utvecklingen av SIS II och om den potentiella migrationen från den första generationens system.[17]

Utvecklingen av **Eurodac** går tillbaka till avskaffandet av de inre gränserna, som gjorde det nödvändigt att tydligt reglera handläggningen av asylansökningar. Eurodac är ett centraliserat och automatiserat system för identifiering av fingeravtryck från vissa tredjelandsmedborgare. Systemet har varit i drift sedan i januari 2003 och fyller en stödfunktion vid fastställandet av vilken medlemsstat som enligt Dublinkonventionen ska bära ansvaret för att handlägga en viss asylansökan.[18] Personer över 14 års ålder som söker asyl i en medlemsstat får per automatik lämna fingeravtryck, och det gäller även tredjelandsmedborgare som grips i samband med att de olagligen försöker passera en yttre gräns. Genom att jämföra dessa personers fingeravtryck med Eurodac-registren, försöker de nationella myndigheterna att fastställa var han eller hon kan ha lämnat in en asylansökan tidigare eller när vederbörande först reste in i Europeiska unionen. Myndigheterna kan också använda sig av Eurodac-registren för att jämföra fingeravtryck från tredjelandsmedborgare som vistas olagligen på deras territorium. Medlemsstaterna ska ange en förteckning över de myndigheter som har tillgång till databasen, vanligtvis asyl- och invandringsmyndigheter, gränsbevakning och polis. Medlemsstaterna överför relevanta uppgifter till den centrala databasen via sina nationella kontaktpunkter. Personuppgifter i Eurodac får endast användas för att underlätta tillämpningen av Dublinkonventionen. All annan användning kan leda till påföljder. Asylsökandes fingeravtryck lagras i tio år, medan fingeravtryck från illegala migranter sparas i två år. Asylsökandes uppgifter raderas när den sökande beviljas medborgarskap i en medlemsstat. Illegala migranters fingeravtryck raderas när de får uppehållstillstånd eller medborgarskap, eller när de lämnar medlemsstaternas territorium. Direktiv 95/46/EG gäller för behandlingen av personuppgifter enligt det här instrumentet.[19] Eurodac, som drivs med hjälp av kommissionens s-Testanätverk, används i alla medlemsstater samt i Norge, Island och Schweiz. Ett avtal som som gör det möjligt för Liechtenstein att ansluta sig väntar på att ingås. Kommissionen ska årligen överlämna rapporter till Europaparlamentet och rådet om driften av Eurodacs centrala enhet.

I efterdyningarna av terrorattackerna den 11 september 2001 beslutade medlemsstaterna att påskynda genomförandet av en gemensam viseringspolitik genom att inrätta en form av informationsutbyte med avseende på viseringar för kortare vistelse.[20] Avskaffandet av de inre gränserna har också bidragit till att underlätta missbruk av vissa medlemsstaters viseringsordningar. **Informationssystemet för viseringar** (VIS) syftar till att ta ett grepp om båda dessa frågor. Det ska således bidra till genomförandet av den gemensamma viseringspolitiken genom att underlätta prövningen av viseringsansökningar och genomförandet av kontroller vid de yttre gränserna, och samtidigt fungera som verktyg för att förebygga hot mot medlemsstaternas inre säkerhet.[21] VIS kommer att vara ett centraliserat

---

17 Rådets förordning (EG) 1104/2008, EUT L 299, 8.11.2008, s. 1; rådets beslut 2008/839/RIF, EUT L 299, 8.11.2008, s. 43.

18 Rådets förordning (EG) nr 343/2003, EUT L 50, 25.2.2003, s. 1 (Dublinförordningen), rådets förordning (EG) 2725/2000, EGT L 316, 15.12.2000, s. 1 (Eurodacförordningen). Dessa rättsakter bygger på 1990 års Dublinkonvention (EGT C 254, 19.8.1997, s. 1), som syftade till att fastställa vilken medlemsstat som hade ansvaret för att pröva asylansökningar. Systemet för prövning av asylansökningar brukar kallas ”Dublinsystemet”.

19 Direktiv 95/46/EG, EGT L 281, 23.11.1995, s. 31.

20 Extrainsatt rådsmöte (rättsliga och inrikes frågor), 20.9.2001.

21 Rådets beslut 2004/512/EG, EUT L 213, 15.6.2004, s. 5; förordning (EG) nr 767/2008, EUT L 218, 13.8.2008, s. 60; rådets beslut 2008/633/RIF, EUT L 218, 13.8.2008, s. 129. Se även Europeiska rådets uttalande om kampen mot terrorismen, 25.3.2004.

informationssystem bestående av en nationell del i varje deltagande stat och en teknisk stödfunktion placerad i Frankrike. Det kommer att använda ett system för biometrisk matchning för att säkerställa tillförlitliga jämförelser av fingeravtryck och kontrollera viseringsinnehavares identitet vid de yttre gränserna. VIS kommer att omfatta uppgifter om viseringsansökningar, fotografier, fingeravtryck, anknytande beslut av viseringsmyndigheter samt länkar mellan ansökningar med ansknytning till varandra. Viserings-, asyl-, invandrings- och gränskontrollmyndigheter kommer att ha tillgång till databasen för att kunna kontrollera viseringsinnehavares identitet och viseringars äkthet. Polisen och Europol får använda basen för att förebygga och bekämpa terrorism och andra former av allvarlig brottslighet.[22] Ansökningshandlingar får sparas i fem år. Personuppgifter i VIS ska behandlas i enlighet med de särskilda bestämmelserna i de grundläggande rättsakter som reglerar detta system (förordning (EG) nr 767/2008 och rådets beslut 2008/633/RIF), som kompletterar bestämmelserna i direktiv 95/46/EG, förordning (EG) nr 45/2001, rådets rambeslut 2008/977/RIF, Europarådets konvention nr 108, dess tilläggsprotokoll nr 181 samt polisrekommendationen.[23] VIS kommer att användas i alla medlemsstater utom Förenade kungariket och Irland, samt i Schweiz, Norge och Island, och fungera på grundval av kommissionens s-Testa-nät. Kommissionen kommer att utvärdera systemet tre år efter det att det tagits i drift och därefter vart fjärde år.

På spanskt initiativ antog rådet 2004 ett direktiv om lufttrafikföretags överföring av **förhandsuppgifter om passagerare** (API) till myndigheter som ansvarar för gränskontroll.[24] Syftet med denna rättsakt är att förbättra gränskontrollen och bekämpa illegal migration. När det gäller passagerare som reser till EU från tredjeländer ska lufttrafikföretagen ska på begäran meddela gränskontrollmyndigheterna passagerarnas namn, födelsedatum, medborgarskap, ort för ombordstigning och gränsövergångsställe för inresa. Sådana uppgifter av personlig karaktär hämtas i normala fall från den maskinläsbara delen av passagerarens pass och vidarebefordras till myndigheterna efter incheckning. Från det att ett flyg har anlänt får myndigheterna och flygbolagen spara passageraruppgifterna i 24 timmar. Det rör sig om ett decentraliserat system som bygger på informationsutbyte mellan privata aktörer och offentliga myndigheter. Rättsakten medger inte utbyte av passageraruppgifter mellan medlemsstater. Andra brottsbekämpande myndigheter än gränsbevakningen kan dock begära att få tillgång till uppgifterna för brottsbekämpningsändamål. Personuppgifter får endast användas av offentliga myndigheter för att säkerställa gränskontroll och bekämpa illegal migration. Behandlingen ska ske i överensstämmelse med direktiv 95/46/EG.[25] Denna rättsakt, som är i kraft i hela EU, tillämpas endast av ett fåtal av medlemsstaterna. Kommissionen avser att se över direktivet under 2011.

En viktig del av kommissionens program 1992, som ledde till inrättandet av den inre marknaden, rörde avskaffandet av alla kontroller och formaliteter för varor som

---

22 Rådets beslut 2008/633/RIF, EUT L 218, 13.8.2008, s. 129.

23 Förordning (EG) nr 767/2008, EUT L 218, 13.8.2008, s. 60; rådets beslut 2008/633/RIF, EUT L 218, 13.8.2008, s. 129; direktiv 95/46/EG, EGT L 281, 23.11.1995, s. 31; förordning (EG) nr 45/2001, EGT L 8, 12.1.2001, s. 1; rådets rambeslut 2008/977/RIF, EUT L 350, 30.12.2008, s. 60; konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 28.1.1981 (Europarådets konvention nr 108); tilläggsprotokoll till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181), Europarådet, 8.11.2001 (tilläggsprotokoll nr 181); Europarådets ministerkommittés relommendation nr R (87) 15 avseende reglering av användningen av personuppgifter inom den polisiära sektorn, Europarådet, 17.9.1987 (polisrekommendationen).

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

25 Direktiv 95/46/EG, EGT L 281, 23.11.1995, s. 31.

transporterades inom gemenskapen.[26] Avskaffandet av dessa förfaranden vid de inre gränserna ledde till en ökad risk för begrägeri, vilket gjorde det nödvändigt för medlemsstaterna att inrätta en mekanism för ömsesidigt administrativt bistånd i syfte att förebygga, utreda och lagföra överträdelser av gemenskapens tull- och jordbrukslagstiftning, dels ett tullsamarbete för att göra det möjligt att avslöja och lagföra överträdelser av nationella tullbestämmelser, särskilt genom att förbättra det gränsöverskridande informationsutbytet. Utan att det påverkar EU:s behörighet i tullunionen[27] syftar **Neapel II-konventionen** om ömsesidigt bistånd och samarbete mellan tulladministrationer till att förebygga och avslöja överträdelser av de nationella tullbestämmelserna och till att hjälpa de berörda myndigheterna att lagföra och bestraffa överträdelser av gemenskapens respektive medlemsstaternas tullagstiftning.[28] Enligt detta instrument är det en grupp av centrala samordningsenheter som skriftligen begär bistånd från sina motsvarigheter i andra medlemsstater i samband med brottsutredningar rörande överträdelse av medlemsstaternas respektive gemenskapens tullbestämmelser. Dessa enheter får endast personuppgifter när det sker för att uppfylla Neapel II-konventionens syften. De kan vidarebefordra sådan information till nationella tullmyndigheter, utredande myndigheter och rättsliga organ samt, under förutsättning att den medlemsstat som lämnat uppgifterna givit sitt samtycke, till andra myndigheter. Uppgifterna kan lagras under en period som inte överstiger vad som krävs för att uppfylla det ändamål för vilket de tillhandahölls. Personuppgifter ska omfattas av åtminstone samma grad av skydd i den mottagande medlemsstaten som i den medlemsstat som har lämnat uppgifterna, och uppgiftsbehandlingen måste vara förenlig med bestämmelserna i direktiv 95/46/EG och Europarådets konvention nr 108.[29] Neapel II-konventionen har ratificerats av samtliga medlemsstater. De har möjlighet att föreslå ändringar av konventionen. Om så sker kan medlemsstaterna ska den nya texten antas av ministerrådet och ratificeras på nytt av medlemsstaterna.

Genom CIS-konventionen, som fungerar som ett komplement till Neapel II-konventionen, infördes **tullinformationssystemet** (TIS) för att bidra till arbetet med att förebygga, utreda och lagföra allvarliga överträdelser av den nationella lagstiftningen. Detta mål ska uppnås genom att man via en snabbt utbyte av information effektiviserar samarbetet mellan medlemsstaternas tullmyndigheter.[30] TIS, som förvaltas av kommissionen, är ett centraliserat informationssystem som kan kontaktas via terminaler i medlemsstaterna och hos kommissionen, Europol och Eurojust. Det omfattar personuppgifter med anknytning till råvaror, transportmedel, företag, personer och varor samt till kvarhållande, beslag eller förverkande av kontanta medel. Personuppgifterna utgörs av namn och antagna namn, födelsedatum och födelseort, medborgarskap, kön, fysiska kännetecken, id-handlingar, adress, tidigare tecken på våldsbenägenhet, skäl till att uppgifterna förs in i TIS, föreslagna åtgärder samt transportmedels registreringsnummer. När det gäller varor och kontanta medel som

---

26 Rådets förordning (EEG) 2913/92, EGT L 302, 19.10.1992.

27 Rådets förordning (EG) nr 515/97 av den 13 mars 1997 om ömsesidigt bistånd mellan medlemsstaternas administrativa myndigheter och om samarbete mellan dessa och kommissionen för att säkerställa en korrekt tillämpning av tull- och jordbrukslagstiftningen, EGT L 82, 22.3.1997, s. 1, ändrad genom förordning (EG) nr 766/2008, EUT L 218, 13.8.2008, s. 48.

28 Konvention upprättad på grundval av artikel K 3 i fördraget om Europeiska unionen om ömsesidigt bistånd och samarbete mellan tullförvaltningar, EGT C 24/2, 23.1.1998 (Neapel II-konventionen).

29 Direktiv 95/46/EG, EGT L 281, 23.11.1995, s. 31; konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 8.11.2001 (Europarådets konvention nr 108).

30 Konvention som utarbetats på grundval av artikel K.3 i Fördraget om Europeiska unionen, om användning av informationsteknologi för tulländamål, EGT C 316, 27.11.1995, s. 34, ändrad genom rådets beslut 2009/917/RIF, EUT L 323, 10.12.2009, s. 20.

kvarhållits, tagits i beslag eller förverkats får endast personuppgifter i snäv bemärkelse föras in i TIS. Sådan information får endast användas för observation och rapportering eller för att utföra särskilda inspektioner eller specifika kontroller av, eller för strategiska eller operativa analyser avseende personer som misstänks ha brutit mot de nationella tullbestämmelserna. Nationella tull-, skatte-, jordbruks-, hälsovårds- och polismyndigheter samt Europol och Eurojust har tillgång till uppgifter i TIS.[31] Behandlingen av personuppgifter måste ske i överensstämmelse med de särskilda regler som fastställs i TIS-konventionen samt besstämmelserna i direktiv 95/46/EG, förordning (EG) nr 45/2001, Europarådets konvention nr 108 och polisrekommendationen.[32] Personuppgifter får endast kopieras från TIS till andra databehandlingssystem för riskhantering eller operativa analyser, dit bara analytiker som utsetts av medlemsstaterna får tillgång. Personuppgifter som kopierats från TIS får bara behållas under den tid som behövs för att nå syftet för vilket de kopierades och högst under tio år. I TIS finns också ett **register för identifiering av tullutredningar** (Fide) för att bidra till att förebygga, utreda och lagföra allvarliga övertädelser av nationell lagstiftning.[33] Fide gör det möjligt för nationella myndigheter ansvariga för att genomföra tullundersökningar, när de inleder en utredning, att identifiera andra myndigheter som kan ha undersökt en given person eller verksamhet. Dessa myndigheter kan föra in uppgifter i Fide från sina utredningar, inklusive biografiska uppgifter om personer som undersöks och bolagsnamn, handelsnamn, momsregistreringsnummer och adress för de verksamheter som undersöks. Uppgifter från utredningar där inga tullbedrägerier har upptäckts får lagras under högst tre år. Uppgifter från utredningar där fall av tullbedrägeri har upptäckts får lagras under högst sex år och uppgifter från utredningar med fällande dom eller sanktion får behållas under högst tio år. TIS och Fide använder det gemensamma kommunikationsnätet, gemensamma systemgränssnittet eller säker webbåtkomst från kommissionen. TIS är tillämpligt i alla medlemstaterna. Kommissionen rapporterar, i samarbete med medlemsstaterna, varje år till Europaparlamentet och rådet om driften av TIS.

EU-instrument som syftar till att förebygga och bekämpa terrorism och andra former av grov gränsöverskridande brottslighet

Terrorattackerna i Madrid 2004 utlöste en rad nu initiativ på EU-nivå. På Europeiska rådets begäran lade kommissionen 2005 fram ett förslag till rättsakt om utbyte av uppgifter enligt principen om tillgänglighet.[34] I stället för att stödja detta förslag antog rådet 2006 det **svenska initiativet**, som underlättar utbytet mellan medlemsstaterna av eventuella befintliga uppgifter

---

31 Från maj 2011 kommer Europol och Eurojust att ha tillgång till CIS på grundval av rådets beslut 2009/917/RIF (EUT L 323, 10.12.2009, s. 20).

32 Konvention som utarbetats på grundval av artikel K.3 i fördraget om Europeiska unionen, om användning av informationsteknologi för tulländamål, EGT C 316, 27.11.1995, s. 34, ändrad genom rådets beslut 2009/917/RIF, EUT L 323, 10.12.2009, s. 20; direktiv 95/46/EG, EGT L 281, 23.11.1995, s. 31; förordning (EG) nr 45/2001, EGT L 8, 12.1.2001, s. 1; konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 181), Europarådet, 28.1.1981 (Europarådets konvention nr 108); Europarådets ministerkommittés relommendation nr R (87) 15 avseende reglering av användningen av personuppgifter inom den polisiära sektorn, Europarådet, 17.9.1987 (polisrekommendationen).

33 FIDE, som står för *Fichier d'Identification des Dossiers d'Enquêtes douanières*, baseras på rådets förordning (EG) nr 766/2008 och det protokoll, inrättat i enlighet med artikel 34 i fördraget om Europeiska unionen, om ändring, när det gäller inrättande av ett register för identifiering av tullutredningar, av konventionen om användning av informationsteknologi för tulländamål, EUT C 139, 13.6.2003, s. 1.

34 KOM(2005) 490, 12.10.2005; ordförandeskapets slutsatser — Haagprogrammet, 4–5.11.2004. Se även Europeiska rådets uttalande om kampen mot terrorismen, 25.3.2004.

eller kriminalunderrättelser som kan vara nödvändiga för en brottsutredning eller en kriminalunderrättelseinsats.[35] Detta instrument bygger på principen om likvärdig tillgång, som innebär att villkoren för gränsöverskridande utbyte av uppgifter inte ska vara strängare än de villkor som tillämpas i den enskilda medlemsstaten. Det svenska initiativet bygger på decentralisering och gör det möjligt för polisen, tullen eller andra myndigheter med befogenheter när det gäller att utreda brott (med undantag för underrättelsetjänster, som vanligtvis hanterar underrättelser med koppling till den nationella säkerheten) att utbyta information och kriminalunderrättelser med sina motsvarigheter i EU. Medlemsstaterna ska utse nationella kontaktpunkter att hantera brådskande förfrågningar om information. Genom denna åtgärd fastställs tydliga tidsfrister för utbytet av information samtidigt som medlemsstaterna åläggs att fylla i ett formulär i samband med att uppgifter begärs. Medlemsstaterna är skyldiga att besvara framställningar om uppgifter och underrättelser inom åtta timmar i brådskande fall, inom en vecka i icke brådskande fall och inom två veckor i alla andra fall. Användningen av uppgifter och underrättelser som erhållits med hjälp av detta instrument regleras av nationella bestämmelser om uppgiftsskydd, med det förbehållet att uppgifter som härrör från andra medlemsstater inte får behandlas annorlunda än information med inhemskt ursprung. En medlemsstat som tillhandahåller uppgifter får dock ställa villkor för användningen av uppgifter eller underrättelser i andra medlemsstater. Personuppgifter ska behandlas i enlighet med nationell lagstiftning om uppgiftsskydd, Europarådets konvention nr 108, dess tilläggprotokoll nr 181 och polisrekommendationen.[36] 12 av de 31 stater som har undertecknat denna åtgärd (inklusive EU-medlemsstater samt Norge, Island, Schweiz och Liechtenstein) har antagit nationell lagstiftning för att genomföra den. Fem stater fyller regelbundet i formuläret för att begära information, men endast två stater använder det mer regelbundet för att utbyta uppgifter.[37] Kommissionen ska lägga fram sin utvärderingsrapport till rådet före utgången av 2010.

Prümbeslutet bygger på ett avtal som Tyskland, Frankrike, Spanien, Beneluxländerna och Österrike ingick 2005 i syfte att intensifiera samarbetet i kampen mot terrorism, gränsöverskridande brottslighet och illegal migration. Som svar på att flera medlemsstater uttryckt intresse av att ansluta sig till detta avtal föreslog Tyskland i samband med sitt ordförandeskap i rådet 2007 att avtalet skulle omvandlas till en EU-rättsakt. I 2008 års Prümbeslut, som ska vara genomfört i augusti 2011, finns bestämmelser om gränsöverskridande utbyte av DNA-profiler, fingeravtryck, uppgifter i fordonsregister och information om personer som misstänks för att planera terrorattacker.[38] Beslutet syftar till att stärka insatserna för att förebygga brott, särskilt terrorism och gränsöverskridande brottslighet, och till att upprätthålla den allmänna ordningen i samband med större idrottsevenemang. Systemet i fråga kommer att vara decentraliserat och är avsett att fungera så att de deltagande staternas databaser för registrering av DNA, fingeravtryck och fordon

---

35 Rådets rambeslut 2006/960/RIF, EUT L 386, 29.12.2006, s. 89.

36 Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 28.1.1981 (Europarådets konvention nr 108); tilläggsprotokoll till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181), Europarådet, 8.11.2001 (tilläggsprotokoll nr 181); Europarådets ministerkommittés relommendation nr R (87) 15 avseende reglering av användningen av personuppgifter inom den polisiära sektorn, Europarådet, 17.9.1987 (polisrekommendationen).

37 Denna information baserar sig på svaren på en enkät. Det spanska ordförandeskapet presenterade resultaten vid ett möte den 22 juni 2010 med den särskilda arbetsgruppen för frågor om informationsutbyte.

38 Rådets beslut 2008/615/RIF, EUT L 210, 6.8.2008, s. 1; rådets beslut 2008/616/RIF, EUT L 210, 6.8.2008, s. 12.

kopplas samman via de nationella kontaktpunkterna. Kontaktpunkterna kommer, med hjälp av kommissionens s-Testanät, att hantera inkommande och utgående framställningar om gränsöverskridande jämförelse av DNA-profiler, fingeravtryck och uppgifter ur fordonsregistret. Deras befogenheter att överföra sådana uppgifter till slutanvändarna regleras av nationell lagstiftning. Från och med augusti 2011 kommer jämförelsen av uppgifter att ske helt automatiskt. Medlemsstaterna måste dock genomgå en mycket sträng granskning (där man bland annat bedömer om uppgiftsskyddet och tekniken uppfyller kraven) för att få tillstånd att inleda det automatiska utbytet av uppgifter. Utbyte av personuppgifter enligt detta instrument får inte ske förrän medlemsstaterna har garanterat ett uppgiftsskydd som åtminstone motsvarar kraven i Europarådets konvention nr 108, dess tilläggsprotokoll nr 181 och polisrekommendationen.[39] Rådet kommer att besluta enhälligt om huruvida detta villkor är uppfyllt. Personuppgifter får endast användas för de ändamål för vilka de tillhandahållits, om inte den tillhandahållande medlemsstaten godkänner att de används för andra ändamål. Enskilda kan också vända sig till sina nationella uppgiftsskyddsombud, som utsetts enligt direktiv 95/46/EG, för att genomdriva sina rättigheter i samband med behandlingen av personuppgifter enligt det här instrumentet. Jämförelsen av DNA-profiler och fingeravtryck kommer att baseras på ett system som anger ”träff” eller ”ingen träff” (anonymt), vilket innebär att myndigheterna endast kan begära personuppgifter om en regisrerad person om deras ursprungliga sökning har resulterat i en träff. Sådana framställningar om ytterligare information kommer i normalfallet att ske i enlighet med det svenska initiativet. Prümbeslutet genomförs i alla 27 EU-medlemsstaterna, medan Norge och Island håller på att ansluta sig till detta samarbete.[40] Kommissionen ska lägga fram sin utvärderingsrapport till rådet 2012.

Efter bombdåden i London i juli 2005 lade Storbritannien, Irland, Sverige och Frankrike fram ett förslag till EU-rättsakt om harmonisering av de nationella bestämmelserna om lagring av uppgifter. I 2006 års **direktiv om lagring av uppgifter** åläggs telefoni- och Internetleverantörer att för vissa ändamål, närmare bestämt att utreda, upptäcka och lagföra allvarlig brottslighet, lagra trafik- och lokaliseringsuppgifter som genereras vid användning av elektroniska kommunikationstjänster samt uppgifter om abonnenter (inklusive deras telefonnummer, IP-adress och IMEI-kod).[41] Direktivet om lagring av uppgifter reglerar varken tillgången till eller användningen av uppgifter som lagras av den nationella myndigheterna. Den elektroniska kommunikationens innehåll undantas uttryckligen från direktivets tillämpningsområde, vilket innebär att avlyssning inte är tillåten enligt denna rättsakt. Enligt direktivet är det upp till medlemsstaterna att definiera ”allvarliga brott”. Medlemsstaterna ska också själva fastställa vilka nationella myndigheter som ska ha tillgång till sådana uppgifter från fall till fall, samt vilka förfaranden och villkor som ska gälla för tillgång till uppgifterna. Lagringsperioderna varierar mellan 6 och 24 månader. Frågor om skydd av personuppgifter som uppkommer vid tillämpningen av direktivet om lagring av

---

39 Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 28.1.1981 (Europarådets konvention nr 108); tilläggsprotokoll till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181), Europarådet, 8.11.2001 (tilläggsprotokoll nr 181); Europarådets ministerkommittés rekommendation nr R (87) 15 avseende reglering av användningen av personuppgifter inom den polisiära sektorn, Europarådet, 17.9.1987 (polisrekommendationen).

40 Hittills har tio medlemsstater fått tillstånd att påbörja det automatiska utbytet av DNA-profiler, medan fem har fått tillstånd för fingeravtryck och sju för uppgifter ur fordonsregister. Tyskland, Österrike, Spanien och Nederländerna har tillhandahållit ofullständig statistik om sin användning av instrumentet.

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

uppgifter regleras av direktiv 95/46/EG och direktiv 2002/58/EG.[42] Sex medlemsstater har ännu inte genomfört denna åtgärd helt och hållet, och författningsdomstolarna i Tyskland respektive Rumänien har förklarat att det nationella genomförandet av denna lagstiftning strider mot författningen. Den tyska författningsdomstolen fann att de nationella bestämmelserna om tillgång till och användning av uppgifter var oförenliga med författningen.[43] Den rumänska författningsdomstolen fann att lagringen av uppgifter *i sig* stred mot artikel 8 i konventionen om skydd av de mänskliga rättigheterna och de grundläggande friheterna (Europeiska konventionen om de mänskliga rättigheterna) och därför var författningsstridig.[44] Kommissionen gör för närvarande en utvärdering av den berörda rättsakten och kommer att lägga fram sin utvärdering till Europaparlamentet och rådet i slutet av 2010.

Det pågående inrättandet av det **europeiska informationssystemet för utbyte av uppgifter ur kriminalregister** (Ecris) går tillbaka på ett belgiskt initiativ från 2004 som syftade till att hindra dömda sexbrottslingar från att arbeta med barn i andra medlemsstater. Medlemsstaterna var tidigare hänvisade till Europarådets konvention om inbördes rättshjälp i brottmål för att kunna utbyta uppgifter om de egna medborgarnas domar, men detta system visade sig vara ineffektivt.[45] Rådet tog det första steget mot en reform genom att anta rådets beslut 2005/876/RIF, som föreskrev att varje medlemsstat skulle inrätta en centralmyndighet med uppgift att regelbundet översända fällande domar mot utländska EU-medborgare till de medlemsstater i vilka personerna i fråga är medborgare.[46] Denna rättsakt innebar också för första gången en möjlighet för medlemsstaterna att, med förbehåll för vad som föreskrivs i den nationella lagstiftningen, få tillgång till tidigare domar som meddelats mot deras egna medborgare i andra medlemsstater. De kunde således begära sådan information genom att fylla i ett standardformulär, i stället för att tillämpa förfaranden för inbördes rättshjälp. Under 2006 och 2007 lade kommissionen fram ett samlat lagstiftningspaket bestående av tre rättsakter: rådets rambeslut 2008/675/RIF som ålägger medlemsstaterna att ta hänsyn till tidigare fällande vid nya brottmålsförfaranden, rådets rambeslut 2009/315/RIF om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll och rådets beslut 2009/316/RIF, varigenom Ecris inrättades som teknisk lösning för att utbyta uppgifter ur kriminalregister.[47] Rådets rambeslut 2009/315/RIF och 2009/316/RIF, som ska vara genomförda senast i april 2012, syftar till att fastställa vilka metoder som ska användas när uppgifter om en ny fällande dom ska överföras från den medlemsstat där domen meddelats till den medlemsstat där den dömde är medborgare, skyldigheterna att lagra uppgifter och en ram för ett datoriserat system för informationsutbyte. Ecris kommer att vara ett decentraliserat informationssystem som knyter samman medlemsstaternas kriminalregister via kommissionens s-Testanätverk. Ett antal centralmyndigheter kommer att utbyta uppgifter om nya domar mot EU-medborgare och om tidigare fällande domar. Uppgifterna kommer att krypteras, struktureras enligt ett fastställt format och omfatta följande information: personuppgifter, dom, påföljd och eventuella förbrott samt kompletterande information

---

42 Direktiv 95/46/EG, EGT L 281, 23.11.1995, s. 31; direktiv 2002/58/EG, EGT L 201, 31.7.2002, s. 37 (direktivet om integritet och elektronisk kommunikation).

43 Avgörande av den tyska författningsdomstolen, Bundesverfassunggericht 1 BvR 256/08, 11.3.2008.

44 Den rumänska författningsdomstolens avgörande nr 1258, 8.10.2009.

45 Europeiska konventionen om inbördes rättshjälp i brottmål (ETS nr 30), Europarådet, 20.4.1959. Se även KOM(2005) 10, 25.1.2005.

46 Rådets beslut 2005/876/RIF, EUT L 322, 9.12.2005, s. 33.

47 Rådets rambeslut 2008/675/RIF, EUT L 220, 15.8.2008, s. 32; rådets rambeslut 2009/315/RIF, EUT L 93, 7.4.2009, s. 23; rådets beslut 2009/316/RIF, EUT L 93, 7.4.2009, s. 33. Se även KOM(2005) 10, 25.1.2005.

(inklusive fingeravtryck, om sådana finns tillgängliga). Från och med april 2012 ska utdrag ur kriminalregister tillhandahållas i pågående brottmål och översändas till rättsliga eller behöriga administrativa myndigheter, till exempel organ som har rätt att utföra personkontroller för känsliga anställningar eller innehav av skjutvapen. Personuppgifter som tillhandahålls i brottmål får endast användas för det avsedda ändamålet. All annan användning kräver samtycke från den medlemsstat som har tillhandahållit uppgifterna. Behandlingen av personuppgifter måste ske i överensstämmelse med de särskilda bestämmelser som infördes med rådets beslut 2009/315/RIF, som införlivar bestämmelserna i rådets beslut 2005/876/RIF, samt rådets rambeslut 2008/977/RIF och Europarådets konvention nr 108.[48] All behandling av personuppgifter som utförs av EU-institutioner som använder Ecris, till exempel för att säkerställa datasäkerheten, omfattas av förordning (EG) 45/2001.[49] Detta lagstiftningspaket innehåller inga bestämmelser om lagring av uppgifter, eftersom lagringen av uppgifter om brottmålsdomar regleras av nationell lagstiftning. Femton medlemsstater deltar för närvarande i ett pilotprojekt, och av dessa har nio inlett ett elektronsikt utbyte av uppgifter hämtade från kriminalregister. Kommissionen ska lägga fram två utvärderingsrapporter om hur lagstiftningspaketet fungerar för Europaparlamentet och rådet: rambeslut 2008/675/RIF ska ses över 2011, rambeslut 2009/315/RIF ska ses över 2015. Från och med 2016 ska kommissionen också regelbundet offentliggöra rapporter om driften av Ecris.

På finskt initiativ antog rådet 2000 ett beslut om organisering av utbytet av uppgifter mellan medlemsstaternas **finansunderrättelseenheter** i syfte att bekämpa penningtvätt och, senare, finansiering av terrorism.[50] Finansunderrättelseenheterna är vanligtvis inrättade inom brottsbekämpande organ, rättsliga myndigheter eller förvaltningsorgan med som rapporterar till finansmyndigheter. De är skyldiga att lämna ut nödvändiga finansiella uppgifter och uppgifter av relevans för brottsbekämpningen, inklusive upplysningar om finansiella transaktioner, med sina motsvarigheter inom EU, utom i sådana fall där utlämnandet av uppgifterna skulle vara en oproportionerlig åtgärd med hänsyn till fysiska eller juridiska personers intressen. Uppgifter som tillhandahållits i syfte att analysera eller utreda penningtvätt eller finansiering av terrorism kan också användas som underlag för brottsutredningar eller åtal i övrigt, såvida inte lagstiftningen i den medlemsstat som tillhandahållit uppgifterna förbjuder sådan användning. Behandlingen av personuppgifter får inte strida mot bestämmelserna i rådets rambeslut 2008/977/RIF, Europarådets konvention nr 108 och polisrekommendationen.[51] Under 2002 inrättade flera medlemsstater FIU.net, ett decentraliserat elektroniskt nätverk som hanterar utbyte av uppgifter mellan finansunderrättelseenheterna och använder kommissionens s-Testanätverk.[52] Tjugo finansunderrättelseenheter har anslutit sig till detta nät. Diskussioner pågår om att använda Europols säkra Sienaprogram för att driva FIU.net.[53] Efter att ha bedömt i vilken utsträckning medlemsstaterna följer denna rättsakt beslutade rådet att i det tredje direktivet om

---

48 Rådets rambeslut 2009/315/RIF, EUT L 93, 7.4.2009, s. 23; rådets beslut 2005/876/RIF, EUT L 322, 9.12.2005, s. 33; rådets rambeslut 2008/977/RIF, EUT L 350, 30.12.2008, s. 60; konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 28.1.1981 (Europarådets konvention nr 108).

49 Förordning (EG) nr 45/2001, EGT L 8, 12.1.2001, s. 1.

50 Rådets beslut 2000/642/RIF, EGT L 271, 24.10.2000, s. 4.

51 Rådets rambeslut 2008/977/RIF, EUT L 350, 30.12.2008, s. 60; konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), Europarådet, 28.1.1981 (Europarådets konvention nr 108); Europarådets ministerkommittés rekommendation nr R (87) 15 avseende reglering av användningen av personuppgifter inom den polisiära sektorn, Europarådet, 17.9.1987 (polisrekommendationen).

52 http://www.fiu.net/

53 Siena står för *Secure Information Exchange Network Application*.

penningtvätt ge finansunderrättelseenheterna att befogenhet att motta, analysera och sprida rapporter om misstänkta transaktioner med anknytning till penningtvätt *och* finansiering av terrorism.[54] Kommissionen har sedan 2009 övervakat genomförandet av det tredje direktivet om penningtvätt, inom ramen för sin handlingsplan för finansiella tjänster.[55]

Genom att ta fasta på ett initiativ som lades fram av Österrike, Belgien och Finland antog rådet 2007 ett instrument som syftar till att förbättra samarbetet mellan **kontoren för återvinning av tillgångar** när det gäller att spåra och identifiera vinning av brott.[56] I likhet med finansunderrättelseenheterna samarbetar kontoren för återvinning av tillgångar decentraliserat, även om deras samarbete inte har någon webbplattform att stödja sig på. Kontoren måste använda det svenska initiativet för att utbyta uppgifter, och när de gör det ska de lämna närmare upplysningar om den berörda egendomen, till exempel bankkonton, fastigheter eller fordon, samt uppgifter om de fysiska eller juridiska personer som tillgångarna ska återvinnas från, inklusive deras namn och adress samt födelsedatum och aktieägare eller bolagsinformation (i förekommande fall). Användningen av uppgifter som utbyts i enlighet med detta instrument omfattas av nationell lagstiftning om uppgiftsskydd, med det förbehållet att medlemsstaterna inte får göra åtskillnad i behandlingen av inhemska uppgifter och uppgifter som härrör från andra medlemsstater. Behandlingen av personuppgifter måste vara förenlig med bestämmelserna i Europarådets konvention nr 108, dess tilläggsprotokoll nr 181 och polisrekommendationen.[57] Hittills har mer än tjugo medlemsstater inrättat kontor för återvinning av tillgångar. Med hänsyn till att uppgifterna i fråga är av känslig natur, pågår diskussioner om att använda Europols Sienasystem för utbytet av uppgifter mellan kontoren för återvinning av tillgångar. I ett pilotprojekt som startades i maj 2010 började tolv kontor för återvinning av tillgångar att utbyta uppgifter av relevans för spårning av tillgångar. Kommissionen ska lägga fram en utvärderingsrapport för rådet 2010.

Under 2008 uppmanade rådets franska ordförandeskap medlemsstaterna att inrätta nationella **plattformar för rapportering om it-brottslighet**, och Europol att skapa en europeisk plattform för rapportering om it-brottslighet, i syfte att samla in, analysera och utbyta uppgifter om brott som begås via Internet.[58] Enskilda medborgare kan rapportera olagligt innehåll eller beteende på Internet till sina nationella plattformar. Den europeiska plattformen för rapportering om it-brottslighet, som förvaltas av Europol, skulle fungera som ett informationsnav där uppgifter som omfattas av Europols mandat analyseras och utbyts med nationella brottsbekämpande myndigheter.[59] Idag har nästa alla medlemsstater inrättat

---

54 Direktiv 2005/60/EG, EUT L 309, 25.11.2005, s. 15 (tredje direktivet om penningtvätt).

55 Se exempelvis *Evaluation of the economic impacts of the Financial Services Action Plan — Final report* (för Europeiska kommissionen, DG MARKT), CRA International, 03.2009.

56 Rådets beslut 2007/845/RIF, EUT L 332, 18.12.2007, s. 103.

57 Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), 28.1.1981 (Europarådets konvention 108); Tilläggsprotokoll till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter med avseende på tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181), Europarådet, 8.11.2001 (tilläggsprotokoll 181); Ministerkommitténs rekommendation R(87) 15 av den 17 september 1987 om polisens användning av personuppgifter , Europarådet, 17.9.1987 (polisrekommendationen).

58 Rådets slutsatser om upprättande av nationella plattformar och en europeisk plattform för rapportering om brott på Internet, rådet (rättsliga och inrikes frågor), 24.10.2008; rådets slutsatser om en handlingsplan för genomförandet av en samordnad strategi för att bekämpa brottslighet, (allmänna frågor), 26.4.2010. Europol kallar sitt projekt för Europeisk plattform mot cyberbrottslighet.

59 Ändamålet med Europol är att förebygga och bekämpa organiserad brottslighet, terrorism och andra former av allvarlig brottslighet som påverkar två eller fler medlemsstater. Se rådets beslut 2009/371/RIF, EUT L 121, 15.5.2009, s. 37.

nationella plattformar för rapportering om it-brottslighet. Europol arbetar på det tekniska genomförandet av sin plattform och kan snart komma att ta sitt Sienasystem i bruk för att förbättra utbytet av uppgifter med de nationella plattformarna. I den utsträckning ett sådant utbyte av uppgifter innebär att Europol kommer att behandla personuppgifter gäller de särskilda bestämmelserna om uppgiftsskydd i Europolbeslutet (rådets beslut 2009/371/RIF) samt förordning (EG) 45/2001, Europarådets konvention nr 108, dess tilläggsprotokoll nr 181 och polisrekommendationen.[60] Bestämmelserna i rådets rambeslut 2008/977/RIF reglerar utbytet av personuppgifter mellan medlemsstaterna och Europol.[61] I avsaknad av en rättsakt finns det ingen formell översynsmekanism för plattformar för rapportering om it-brottslighet. Europol har dock redan sett till att täcka detta viktiga område och kommer i framtiden att rapportera om plattformarnas verksamhet i sin årliga rapport, som läggs fram för rådet för godkännande och översänds till Europaparlamentet för kännedom.

EU-byråer och EU-organ som har i uppdrag att bistå medlemsstaterna när det gäller att förebygga och bekämpa allvarlig gränsöverskridande brottslighet

Europeiska polisbyrån (Europol), som inrättades 1995, påbörjade sin verksamhet 1999 och blev ett EU-organ i januari 2010.[62] Byrån ska stödja medlemsstaterna i deras arbete med att förebygga och bekämpa organiserad brottslighet, terrorism och andra former av allvarlig brottslighet som berör två eller flera medlemsstater. Till dess viktigaste uppgifter hör att samla in, lagra, behandla, analysera och utbyta information och underrättelser, att underlätta utredningar samt att förse medlemsstaterna med underrättelser och analytiskt stöd. Den viktigaste förbindelselänken mellan Europol och medlemsstaterna är Europols nationella enheter, som stationerar ut sambandsmän till Europol. Cheferna för de nationella enheterna sammanträder regelbundet för att bistå Europol i operativa frågor, medan Europols styrelse och direktör utövar tillsyn över byråns funktion. Bland Europols verktyg för informationshantering finns Europols informationssystem, analysregister och Sienasystemet. Europols informationssystem innehåller information av personuppgiftskaraktär om personer som misstänks för brott som omfattas av Europols mandat, till exempel biometriska kännetecken, tidigare brottmålsdomar och kopplingar till organiserad brottslighet. Tillgången till dessa uppgifter är begränsad till Europols nationella enheter, sambandsmän, bemyndigad Europolpersonal samt direktören. Analysregistren, som upprättades för att användas vid brottsutredningar, omfattar uppgifter om enkilda och all annan information som Europols nationella enheter beslutar att föra in. Uppgifterna är tillgängliga för sambandsmännen, men endast Europols analytiker får föra in uppgifter. En indexfunktion för det möjligt för de nationella enheterna och sambandsmännen att kontrollera huruvida ett analysregister innehåller uppgifter av intresse för deras medlemsstat. Medlemsstaterna använder sig i allt större utsträckning av Europols Sienasystem för att utbyta känsliga uppgifter för brottsbekämpningsändamål. Europol får behandla information och underrättelser, inklusive

---

60 Rådets beslut 2009/371/RIF, EUT L 121, 15.5.2009, s. 37; förordning (EG) nr 45/2001, EGT L 8, 12.1.2001, s. 1; Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), 28.1.1981 (Europarådets konvention 108); tilläggsprotokoll till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter med avseende på tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181), Europarådet, 8.11.2001 (tilläggsprotokoll 181); ministerkommitténs rekommendation R(87) 15 av den 17 september 1987 om polisens användning av personuppgifter , Europarådet, 17.9.1987 (polisrekommendationen).

61 Rådets rambeslut 2008/977/RIF, EUT L 350, 30.12.2008, s. 60.

62 Rådets beslut 2009/371/RIF, EUT L 121, 15.5.2009, s. 37, som ersätter konventionen baserad på artikel K.3 i fördraget om Europeiska unionen, om upprättandet av en europeisk polisbyrå, EGT C 316, 27.11.1995, s. 2.

personuppgifter, vid utförandet av uppdrag. Medlemsstaterna får endast använda information som hämtats från Europols register för att förebygga och bekämpa allvarlig brottslighet av gränsöverskridande karaktär. Om en medlemsstat som lämnar information meddelar begränsningar för hur denna information får användas, ska dessa begränsningar även gälla andra användare som hämtar sådana uppgifter från Europols register. Europol har också rätt att utbyta personuppgifter med tredjeländer som har ingått operativa avtal med Europol och som garanterar en tillräcklig skyddsnivå för uppgifterna. Europol får lagra uppgifter så länge som behövs för att Europol ska kunna fullgöra sitt uppdrag. Ansalysregister får bevaras i högst tre år, med möjlighet till tre års förlängning. Europols behandling av personuppgifter måste vara förenlig med de särskilda bestämmelserna om uppgiftsskydd i rådets beslut 2009/371/RIF) samt med förordning (EG) 45/2001, Europarådets konvention nr 108, dess tilläggsprotokoll nr 181 och polisrekommendationen.[63] Bestämmelserna i rådets rambeslut 2008/977/RIF ska tillämpas på utbytet av personuppgifter mellan medlemsstaterna och Europol.[64] En gemensam tillsynsmyndighet, bestående av företrädare för de nationella tillsynsmyndigheterna, ska övervaka Europols behandling av personuppgifter och dess översändande av personuppgifter till andra parter. Den gemensamma tillsynsmyndigheten ska regelbundet överlämna rapporter tll Europaparlamentet och rådet. Europol ska ge in en årlig verksamhetsrapport till rådet för godkännande och till Europaparlamentet för kännedom.

Utöver verkningarna med avseende på flera rättsakter som beskrivits ovan ledde terrorattackerna den 11 september 2001 till att **Europeiska unionens enhet för rättsligt samarbete** (Eurojust) inrättades 2002.[65] Eurojust är ett EU-organ som har till mål att förbättra samordningen av utredningar och åtal i medlemsstaterna och att stärka samarbetet mellan de behöriga nationella myndigheterna. Enheten arbetar med samma typer av brott som Europol. Inom ramen för sitt uppdrag och för att kunna utföra sina uppgifter har Eurojusts 27 medlemmar, som tillsammans utgör dess kollegium, tillgång till personuppgifter om misstänkta och tilltalade. Sådana uppgifter omfattar bland annat följande: uppgifter om personens bakgrund, kontaktuppgifter, uppgifter ur fordonsregister, DNA-profiler, fotografier, fingeravtryck, men även trafik- och lokaliseringsuppgifter samt uppgifter om abonnenter som tillhandahålls av leverantörer av telekommunikationstjänster. Medlemsstaterna förväntas dela sådan information med Eurojust så att enheten kan fullgöra sina uppgifter. Ärenderelaterade personuppgifter ska införas via Eurojusts automatiska system för ärendehantering (*case management system*), som drivs via kommissionens s-Testa-nätverk. Personuppgifter och andra uppgifter av relevans för pågående utredningar lagras i ett särskilt register. Eurojust har rätt att behandla personuppgifter inom ramen för sitt mandat, men dessa åtgärder måste vara förenliga med de särskilda bestämmelserna i rådets beslut 2009/426/RIF samt med Europarådets konvention nr 108, dess tilläggsprotokoll nr 181 och polisrekommendationen. Bestämmelserna i rådets rambeslut 2008/977/RIF ska tillämpas på utbytet av personuppgifter mellan medlemsstaterna och Eurojust.[66] Eurojust får utbyta uppgifter med nationella

---

63 Rådets beslut 2009/371/RIF, EUT L 121, 15.5.2009, s. 37; förordning (EG) nr 45/2001, EGT L 8, 12.1.2001, s. 1; Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), 28.1.1981 (Europarådets konvention 108); Tilläggsprotokoll till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter med avseende på tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181), Europarådet, 8.11.2001 (tilläggsprotokoll 181); Ministerkommitténs rekommendation R(87) 15 av den 17 september 1987 om polisens användning av personuppgifter , Europarådet, 17.9.1987 (polisrekommendationen)

64 Rådets rambeslut 2008/977/RIF, EUT L 350, 30.12.2008, s. 60.

65 Rådets beslut 2002/187/RIF, EGT L 63, 6.3.2002, s. 1, ändrat genom rådets beslut 2009/426/RIF, EUT L 138, 4.6.2009, s. 14. Se även det extrainsatta rådsmötet (rättsliga och inrikes frågor) den 20.9.2001.

66 Rådets rambeslut 2008/977/RIF, EUT L 350, 30.12.2008, s. 60.

myndigheter och tredjeländer med vilka avtal har ingåtts, förutsatt att den nationella medlem som har fört in uppgifterna ger sitt samtycke till detta och det berörda tredjelandet kan garantera ett tillräckligt skydd för personuppgifterna. Personuppgifter får lagras så länge som krävs med hänsyn till syftet med registreringen, men måste raderas så snart ett ärende har avslutats. Medlemsstaterna ska ha genomfört den ändrade rättsliga grunden för Eurojust senast i juni 2011. I juni 2014 ska kommissionen se över utbytet av uppgifter mellan de nationella medlemmarna i Eurojust och kan i samband med detta komma att föreslå de förändringar av systemet som den anser lämpliga. I juni 2013 ska Eurojust rapportera till rådet och kommissionen om erfarenheterna av att ge tillgång på nationell nivå till sitt system för ärendehantering. Det ger underlag för medlemsstaterna att se över åtkomsträttigheterna på nationell nivå. En gemensam tillsynsmyndighet, bestående av domare som utsetts av medlemsstaterna, övervakar Eurojusts behandling av personuppgifter och rapporterar årligen till rådet. Kollegiets ordförande ska överlämna en årsrapport om Eurojusts verksamhet till rådet, varpå rådet vidarebefordrar rapporten till Europaparlamentet.

Internationella avtal som syftar till att förebygga och bekämpa terrorism och andra former av allvarlig gränsöverskridande brottslighet

Terrorattackerna den 11 september 2001 ledde till att Förenta staterna antog lagstiftning om att lufttrafikföretag med trafik till, från eller genom dess territorium ska tillhandahålla de amerikanska myndigheterna med **passageraruppgifter** (PNR-uppgifter) som lagras i deras automatiska reservationssystem. Snart beslutade Kanada och Australien att göra samma sak. Eftersom den berörda EU-lagstiftningen förutsätter en förhandsbedömning av det uppgiftsskydd som garanteras av tredjeländer, trädde kommissionen in och förhandlade om så kallade PNR-avtal med dessa länder.[67] Avtalet med Förenta staterna undertecknades i juli 2007, avtalet med Australien i juni 2008 och ett API/PNR-avtal med Kanada i oktober 2005.[68] Avtalen med Förenta staterna respektive Australien är provisoriskt tillämpliga, medan avtalet med Kanada fortsätter att vara i kraft trots att kommissionens beslut om huruvida Kanadas uppgiftsskyddsnormer uppfyller kraven upphörde att gälla i september 2009.[69] Europaparlamentet, som uttryckt missnöje med normernas innehåll, har uppmanat kommissionen att omförhandla alla tre avtalen på grundval av en uppsättning klara principer.[70] PNR-uppgifter som översänds i god tid före en flygavgång hjälper de brottsbekämpande myndigheterna att kontrollera huruvida passagerarna har några kopplingar till terrorism och andra former av allvarlig brottslighet. Syftet med respektive avtal är således att förebygga och bekämpa terrorism och andra former av allvarlig gränsöverskridande brottslighet. I utbyte mot PNR-uppgifter från EU delar Förenta staternas *US Department of Homeland Security* (DHS) med sig av så kallade terroristledtrådar från sina PNR-analyser till brottsbekämpande myndigheter i EU och till Europol och Eurojust. Både Kanada och Förenta staterna har i sina respektive avtal åtagit sig att samarbeta med EU i dess strävan att inrätta ett

---

67 Direktiv 95/46/EG (dataskyddsdirektivet), EGT L 281, 23.11.1995, s. 31.

68 Det kanadensiska paketet består av ett kandadensiskt åtagande rörande behandlingen av API/PNR-uppgifter, kommissionens beslut om huruvida Kanadas uppgiftsskyddsnormer uppfyller kraven samt ett ett internationellt avtal (se EUT L 91, 29.3.2006, s. 49; EUT L 82, 21.3.2006, s. 14). Avtalet med Förenta staterna återfinns i EUT L 204, 4.8.2007, s. 16; avtalet med Australien återfinns i EUT L 213, 8.8.2008, s. 47.

69 Kanada gjorde 2009 ett åtagande genetemot kommissionen, rådets ordförandeskap och EU-medlemsstaterna om att fortsätta tillämpa sitt tidigare åtagande från 2005 rörande användningen av passageraruppgifter från EU. Kommissionens beslut om uppgiftsskyddsnormernas status baserades på detta tidigare åtagande.

70 Europaparlamets resolution, P7_TA(2010)0144, 5.5.2010.

eget PRN-system. Förenta staternas och Australiens avtal omfattar 19 olika kategorier av uppgifter, bland annat biografiska uppgifter, reservation, betalningsinformation och kompletterande uppgifter. Det kanadensiska avtalet omfattar 25 liknande uppgiftskategorier. Till de kompletterande uppgifterna hör uppgifter på enkelbiljetter samt uppgifter om passagerare på väntelista och passagerare som inte dyker upp. Avtalet med Förenta staterna medger också på särskilda villkor användning av känslig information. DHS får behandla sådana uppgifter om det föreligger en risk för den registrerade eller andra, men måste radera uppgifterna inom 30 dagar. PNR-uppgifter överförs till ett antal centrala enheter inom DHS, *Canada Border Services Agency* och den australiensiska tullen, som i sin tur kan överföra uppgifterna till andra inhemska myndigheter med ansvar för brottsbekämpning eller insatser mot terrorism. I avtalet med Förenta staterna förväntar sig DHS inte att den uppgiftsskyddsnivå den ska tillämpa på behandlingen av PNR-uppgifter med ursprung i EU ska vara striktare än den som EU:s myndigheter tillämpar i sina inhemska PNR-system. Om inte denna uppnås kan DHS upphäva vissa delar av avtalet. EU anser att Kanada och Australien ger en tillräcklig skyddsnivå för PNR-uppgifter med ursprung i EU om de uppfyller villkoren i sina respektive avtal. I Förenta staterna behålls PNR-uppgifter från EU under sju år i en aktiv databas och under ytterligare åtta år i en vilande databas. I Australien förs de in i en aktiv databas under 3,5 år och sedan i en vilande databas under två år. I båda länderna gäller att den vilande databasen bara är tillgänglig genom särskilt tillstånd. I Kanada behålls uppgifterna under 3,5 år, men uppgifterna blir anonyma efter 72 timmar. Vart och ett av avtalen ses över regelbundet, men avtalen med Kanada och Australien också innehåller en upphävningsklausul. I EU är det bara Förenade kungariket som har ett PNR-system. Frankrike, Danmark, Belgien, Sverige och Nederländerna har endera antagit relevant lagstiftning eller håller för närvarande på att testa tillämpningen av PNR-uppgifter som en förberedelse inför införandet av PNR-system. Flera andra medlemsstater överväger att införa PNR-system och samtliga medlemsstater använder då och då PNR-uppgifter i brottsbekämpande syfte.

Efter attackerna den 11 september 2001 utarbetade Förenta staternas finansdepartement ett **program för att att spåra finansiering av terrorism** (TFTP) i syfte att identifiera, spåra och lagföra terrorister och personer som stöder terroristerna ekonomiskt. Inom ramen för TFTP använde sig det amerikanska finansministeriet av administrativa förelägganden för att få den amerikanska filialen till ett belgiskt företag att överföra begränsade mängder uppgifter om finansiella meddelanden som passerar genom företagets nät. I januari 2010 ändrade företaget sin systemarkitektur, vilket minskade den mängd uppgifter som omfattas av amerikansk lagstiftning som i normala fall kan bli föremål för administrativa förelägganden från det amerikanska finansdepartementet med mer än hälften. I november 2009 undertecknade ordförandeskapet för Europeiska unionens råd och Förenta staternas regering ett interimsavtal om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från EU till Förenta staterna i syfte att spåra finansiering av terrorism. Avtalet godkändes dock inte av Europaparlamentet.[71] På grundval av ett nytt mandat förhandlade kommissionen om ett nytt utkast till avtal med Förenta staterna, och lade den 18 juni 2010 fram ett förslag till rådsbeslut om ingående av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP-avtalet mellan EU och Förenta staterna).[72] Europaparlamentet gav sitt

[71] Europaparlamets resolution, P7_TA(2010)0029, 11.2.2010.

[72] KOM(2010) 316 slutlig/2, 18.6.2010.

samtycke till ingåendet av avtalet den 8 juli 2010.[73] Rådet väntas nu anta ett rådsbeslut om avtalets ingående, varefter avtalet träder i kraft via ett utbyte av skrivelser mellan de två parterna. Syftet med TFTP-avtalet mellan EU och Förenta staterna är att förebygga, utreda, upptäcka och lagföra terrorism och finansiering av terrorism. Genom avtalet åläggs de utsedda tillhandahållarna av tjänster avseende finansiella betalningsmeddelanden att, på grundval av specifika geografiska hotbedömningar och skräddarsydda framställningar, överföra vissa uppgifter om finansiella betalningsmeddelanden. Det rör sig bland annat om avsändarens och mottagarens namn, kontonummer, adress och identifikationsnummer. Det amerikanska finansministeriet får endast göra sökningar på sådana uppgifter om syftet är att spåra finansiering av terrorism, och det måste dessutom finnas skäl att misstänka att en identifierad person har kopplingar till terrorism eller finansiering av terrorism. Datautvinning och överföring av uppgifter om transaktioner inom det gemensamma eurobetalningsområdet är förbjudet. Förenta staterna meddelar EU-medlemsstaterna, Europol och Eurojust eventuella ”terroristledtrådar” om potentiella terrorhot i EU och kommer att hjälpa EU att inrätta ett eget system som motsvarar TFTP. Om EU skulle inrätta ett sådant program kan båda sidor justera villkoren i avtalet. Innan några uppgifter kan överföras ska varje amerikansk framställan om uppgifter granskas av Europol för att säkerställa att den uppfyller avtalsvillkoren. Information som hämtats från finansiella meddelanden får inte lagras längre än vad som krävs för specifika utredningar eller åtal. Icke framtagna uppgifter får lagras i upp till fem år. Om det krävs för att utreda, förebygga eller lagföra terrorism eller finansiering av terrorism kan finansministeriet överföra alla typer av personuppgifter som hämtats från finansiella betalningsmeddelanden till amerikanska myndigheter med ansvar för brottsbekämpning, allmän säkerhet och insatser mot terrorism samt till EU-medlemsstaterna, Europol eller Eurojust. Det amerikanska finansministeriet kan också dela med sig av eventuella terroristledtrådar rörande EU-medborgare och personer bosatta i EU, förutsett att den berörda medlemsstaten går med på detta. Parternas respekt för den strikta ändamålsbegränsning som innebär att uppgifterna endast får användas för terrorismbekämpning samt övriga säkerhetsåtgärder övervakas av oberoende tillsynsansvariga och av en person som utses av kommissionen. Det löper över fem år och kan sägas upp eller upphävas tillfälligt av endera parten. En tillsynsgrupp från EU ledd av kommissionen och som inbegriper företrädare från två dataskyddmyndigheter och en person från rättsväsendet kommer att se över avtalet sex månader efter ikraftträdandet, och därvid särskilt bedöma parternas tillämpning av avtalets ändamålsbegränsning och proportionalitetsbestämmelser samt deras efterlevnad av bestämmelserna om uppgiftsskydd. Kommissionens rapport kommer att läggas fram för Europaparlamentet och rådet.

2.2. Initiativ enligt handlingsplanen för att genomföra Stockholmsprogrammet

Lagförslag som ska läggas fram av kommissionen

I Stockholmsprogrammet uppmanades kommissionen av Europeiska rådet att lägga fram tre förslag av direkt relevans för detta meddelande: ett unionssystem för passageraruppgifter (PNR) för att göra det möjligt att förebygga, upptäcka och lagföra terrorism och allvarlig brottslighet, ett inrese-/utresesystem och program för registrerade resenärer. Europeiska rådet underströk att de två senare borde tas i drift så snart som möjligt. Kommissionen har tagit fasta på samtliga dessa förslag i sin handlingsplan för att genomföra

[73] Europaparlamentets resolution, P7 TA-PROV(2010)0279, 8.7.2010.

Stockholmsprogrammet.[74] Den kommer nu att sträva efter att genomföra önskemålen och, i framtiden, utvärdera de berörda instrumenten på grundval av de strategier för strategiutveckling som anges i avsnitt 4.

I november 2007 lade kommissionen fram ett förslag till rådets rambeslut användande av passageraruppgifter (PNR-uppgifter) i brottsbekämpningssyfte.[75] Detta initiativ fick stöd i rådet och ändrades senare för att ta hänsyn till Europaparlamentets förslag till ändringar och europeiska datatillsynsmannens synpunkter. När Lissbonfördraget trädde i kraft blev detta förslag inaktuellt. Som framgår av handlingsplanen för Stockholmsprogrammet arbetar kommissionen nu för att i början av 2011 kunna lägga fram ett **PNR-paket** bestående av följande: ett meddelande om en EU-extern PNR-strategi som tar upp de grundläggande principer som ska gälla vid avtalsförhandlingar med tredjeländer, förhandlingsdirektiv för omförhandling av PNR-avtalen med Förenta staterna och Australien samt förhandlingdirektiv för ett nytt avtal med Kanada. Kommissionen är också i färd med att förbereda ett nytt EU-förslag om PNR.

Under 2008 lade kommissionen fram en rad förslag för att utveckla EU:s integrerade gränsförvaltning genom att underlätta resandet för tredjelandsmedborgare och samtidigt förbättra den inre säkerheten.[76] Efter att ha konstaterat att den största gruppen illegala migranter i EU utgörs av personer som stannar kvar längre än de har rätt till, tar kommissionen upp möjligheten att införa ett **system för in- och uttresa** för tredjelandsmedborgare som reser in i EU för kortare vistelser på upp till tre månader. Detta skulle registrera tid och plats för inresan och den tillåtna vistelsens varaktighet samt automatiskt skicka varningar till de behöriga myndigheterna när en person konstaterats ”stanna på övertid”. På grundval av kontroller av biometriska uppgifter skulle det stödjas av samma biometriska matchningssystem och operationella utrustning som används i SIS II och VIS. Kommissionen är för närvarande i färd med att genomföra en konsekvensanalys och kommer, såsom anges i handlingsplanen för genomförande av Stockholmspogrammet, att lägga fram ett förslag till lagstiftning 2011.

Ett **program för registrerade resenärer** (RTP) var det tredje förslaget som togs under övervägande.[77] Detta program skulle göra det möjligt för vissa grupper av personer från tredjeländer som reser ofta att, efter lämpliga kontroller, resa in i EU med förenklade gränskontroller och automatiserade grindar. Ett sådant program skulle också vara baserat på identitetskontroll med hjälp av biometriska uppgifter och göra det möjligt att succesivt frångå den nuvarande strategin, som bygger på generella gränskontroller, och gå mot ett system som baseras på individuell risk. Kommissionen har utfört en konsekvensanalys och har för avsikt att, i enlighet med handlingsprogrammet för genomförande av Stockholmsprogrammet, lägga fram ett lagförslag 2011.

Initiativ som kommissionen ska granska

I Stockholmsprogrammet uppmanades kommissionen av Europeiska rådet att undersöka tre initiativ av relevans för detta meddelande: möjligheterna att spåra finansiering av terrorism i

---

74 Stockholmsprogrammet — ett öppet och säkert europa i medborgarnas tjänst och för deras skydd, rådets dokument 5731/10, 3.3.2010, KOM(2010) 171, 20.4.2010 (Handlingsplan för att genomföra Stockholmsprogrammet).

75 KOM(2007) 654, 6.11.2007.

76 KOM(2008) 69, 13.2.2008.

77 KOM(2008) 69, 13.2.2008.

EU, möjligheterna att utveckla ett europeiskt system för resetillstånd och nyttan med ett sådant projekt samt behovet och mervärdet av att inrätta ett europeiskt polisregistersystem. Kommissionen tog också upp dessa initiativ i handlingsplanen för genomförande av Stockholmsprogrammet. Den kommer nu att bedöma huruvida initiativen kan genomföras och besluta om och hur arbetet ska drivas vidare på grundval av de principer för utarbetande av strategier som beskrivs i avsnitt 4.

I TFTP-avtalet mellan EU och Förenta staterna uppmanas Europeiska kommissionen att undersöka möjligheterna att införa ett **EU-program för att spåra finansiering av terrorism** som motsvarar det amerikanska programmet, vilket skulle möjliggöra en mer riktad överföring av uppgifter från till Förenta staterna.[78] I utkastet till rådsbeslutet om ingående av detta avtal uppmanas kommissionen att till Europaparlamentet och rådet, senast ett år efter det att TFTP-avtalet mellan EU och Förenta staterna trätt i kraft, lägga fram ett rättsligt och tekniskt regelverk för framtagning av uppgifter inom EU:s territorium. Inom tre år efter det att detta avtal har trätt i kraft ska kommissionen lägga fram en lägesrapport om utvecklingen av ett sådant likvärdigt EU-system. Om ett sådant system inte har inrättats inom fem år efter det att avtalet trädde i kraft kan EU besluta sig för att upphäva avtalet. TFTP-avtalet mellan EU och Förenta staterna ålägger också Förenta staterna att samarbeta med EU och bistå med stöd och råd om EU skulle besluta att inrätta ett sådant system. Utan att föregripa ett eventuellt beslut i saken har kommissionen börjat överväga vilka följder dessa planer kan komma att innebära för dataskyddet, i resurshänseende och rent praktiskt. Som anges i handlingsplanen för genomförande av Stockholmsprogrammet kommer kommissionen att under 2011 lägga fram ett meddelande om förutsättningarna för att införa ett EU-program för att spåra finansiering av terrorism (EU-TFTP).

I sitt meddelande från 2008 om integrerad gränsförvaltning tog kommissionen upp möjligheten att införa ett **elektroniskt system för resetillstånd** (ESTA) för tredjelandsmedborgare som inte omfattas av viseringskrav.[79] Enligt detta program skulle tredjelandsmedborgare som uppfyller kraven uppmanas att fylla i en elektronisk ansökan om resetillstånd innan resan påbörjas, och då tillhandahålla passuppgifter och uppgifter om den planerade resan. I jämförelse med viseringsförfarandet skulle det elektroniska systemet för resetillstånd erbjuda ett snabbare och enklare sätt att kontrollera huruvida en person uppfyller de nödvändiga villkoren för inresa. Kommissionen genomför för närvarande en undersökning om fördelar, nackdelar och praktiska konsekvenser av att införa ESTA. Som anges i handlingsplanen för att genomföra Stockholmsprogrammet, är avsikten att under 2011 att lägga fram ett meddelande om förutsättningarna för att införa ett sådant elektronsiskt system för resetillstånd.

Under det tyska ordförandeskapet i rådet 2007 initierade Tyskland en diskussion om huruvida man borde inrätta ett **europeisk polisregistersystem** (Epris).[80] Epris skulle vara till hjälp för tjänstemän vid de brottsbekämpande myndigheterna vid sökandet efter information i EU, särskilt uppgifter som rör förbindelser mellan individer som misstänks för organiserad brottslighet. Kommissionen kommer under 2010 att lägga fram ett utkast till direktiv för en genomförbarhetsstudie rörande Epris. Som anges i handlingsplanen för att genomföra

---

78 Rådets dokument 11222/1/10 REV 1, 24.6.2010, rådets dokument 11222/1/10 REV 1 COR1, 24.6.2010.

79 KOM(2008) 69, 13.2.2008.

80 Se rådets dokument 15526/1/09, 2.12.2009.

Stockholmsprogrammet är avsikten att under 2012 lägga fram ett meddelande om förutsättningarna för att införa ett sådant system.

3. ANALYS AV RÄTTSAKTER SOM TILLÄMPAS, HÅLLER PÅ ATT GENOMFÖRAS ELLER ÖVERVÄGS

Vad som sagts ovan föranleder följande preliminära iakttagelser:

Decentraliserad struktur

Av de olika instrument som för närvarande gäller eller är under genomförande eller övervägande är det endast sex som rör insamling eller lagring av personuppgifter på EU-nivå, nämligen rättsakterna om SIS (och SIS II), VIS, Eurodac, CIS, Europol och Eurojust. Alla andra åtgärder syftar till att reglera det centraliserade, gränsöverskridande utbytet eller överföringen till tredjeländer av personuppgifter som samlats in på nationell nivå av offentliga myndigheter eller privata företag. Den största delen av personuppgifterna samlas in och lagras nationellt. EU strävar efter att tillföra ett mervärde genom att göra det möjligt att på vissa villkor utbyta såda information med EU-partner och tredjeländer. Kommissionen har nyligen lagt fram ett ändrat förslag om inrättande av en byrå för den operativa förvaltningen av stora it-system inom området med frihet, säkerhet och rättvisa för Europaparlamentet och rådet.[81] Den framtida IT-byrån kommer att ha till uppgift att ansvara för den operativa förvaltningen av SIS II, VIS och Eurodac samt andra framtida IT-system inom området med frihet, säkerhet och rättvisa, så att man kan ha dessa system i drift permanent och därigenom garantera ett oavbrutet informationsflöde.

Ändamålsbegränsning

Flera av de instrument som analyserats ovan har ett enhetligt ändamål: Eurodac syftar till att förbättra Dublinsystemets funktion, API till att stärka gränskontrollen, det svenska initiativet till att effektivisera brottsutredningar och underrättelseinsatser, Neapel II-konventionen till att förebygga, avslöja, utreda och lagföra allvarliga överträdelser av den nationella lagstiftningen genom att effektivsera samarbetet mellan de nationella tullmyndigheterna; Ecris, finansunderrättelseenheterna och de nationella kontoren för återvinning av tillgångar till att effektivisera det gränsöverskridande utbytet av uppgifter inom vissa områden; och Prümbeslutet, direktivet om lagring av uppgifter, TFTP och PNR till att bekämpa terrorism och allvarlig brottslighet. SIS, SIS II och VIS framstår som de viktigaste avvikelserna från detta mönster. Det ursprungliga syftet med VIS var att underlätta det gränsöverskridande utbytet av viseringsuppgifter, men det utvidgades senare till att omfatta insatser för att förebygga och bekämpa terrorism och allvarlig brottslighet. SIS och SIS II syftar till att garantera en hög nivå av säkerhet inom området med frihet, säkerhet och rättvisa, och till att underlätta rörligheten för personer som använder uppgifter som meddelats via detta system. Med undantag för dessa centraliserade informationssystem tycks ändamålsbegränsning spela en mycket viktig roll vid utformningen av EU-åtgärder rörande informationsbehandling.

Möjliga överlappningar när det gäller funktionen

Samma personuppgifter kan samlas in på grundval av flera olika instrument, men de får bara användas för de begränsade ändamål som är specifika för respektive instrument (med

[81] KOM(2010) 93, 19.3.2010.

undantag för VIS, SIS och SIS II). En persons biografiska uppgifter, inklusive vederbörandes namn, födelsedatum och födelseort samt medborgarskap, kan exempelvis behandlas i enlighet med SIS, SIS II, VIS, API, CIS, det svenska initiativet, Prümbeslutet, Ecris, finansunderrättelseenheterna, kontoren för återvinning av tillgångar, Europol, Eurojust och PNR- och TFTP-avtalen. Sådana uppgifter kan emellertid endast behandlas för gränskontrolländamål när det gäller API; för att förebygga, utreda och lagföra tullbedrägeri när det gäller CIS; för brottsutredningar och underrättelseinsatser när det gäller det svenska initiativet; för att förebygga terrorism och gränsöverskridande brottslighet när det gäller Prümbeslutet; för att undersöka en persons brottsliga bakgrund när det gäller Ecris; för att utreda en persons kopplingar tuill organiserad brottslighet och terroristnätverk när det gäller finansunderrättelseenheterna; för att spåra tillgångar när det gäller kontoren för återvinning av tillgångar; för att utreda och bidra till lagförinen av allvarlig gränsöverskridande brottslighet när det gäller Europol och Eurojust; för att förebygga och bekämpa terrorism och andra former av allvarlig gränsöverskridande brottslighet när det gäller PNR och; för att identifiera och lagföra terrorister och deras finansiärer när det gäller TFTP. Biometriska uppgifter, i form av exempelvis fingeravtryck och fotografier, kan behandlas i enlighet med SIS II, VIS, Eurodac, det svenska initiativet, Prümbeslutet, Ecris, Europol och Eurojust — men återigen endast inom de ramar som gäller för respektive åtgärd. Prümbeslutet är det enda instrumentet som medger ett gränsöverskridande utbyte av anonymiserade DNA-profiler (även om sådana uppgifter även kan överföras till Europol och Eurojust). Andra system innebär behandling av mycket specifika personuppgifter som endast är av relevans för sina unika ändamål: PNR-systemen behandlar uppgifter om passagerares flygreservationer; FIDE uppgifter av betydelse för utredningen av tullbedrägerier; direktivet om lagring av uppgifter IP-adresser och IMEI-koder; Ecris kriminalregister; kontoren för återvinning av tillgångar privata tillgångar och företagsuppgifter; plattformar för bekämpning av IT-brottslighet IT-brott; Europol kopplingar till kriminella nätverk och TFTP-uppgifter om finansiella meddelanden. Det gränsöverskridande utbytet av uppgifter och underrättelser för brottsutredningsändamål är det enda exemplet på en betydande överlappning när det gäller funktioner. Från en rättslig synvinkel skulle det svenska initiativet vara tillräckligt för att utbyta *alla* typer av uppgifter av relevans för sådana utredningar (förutsatt att utbytet av sådana personuppgifter är tillåtet enligt den nationella lagstiftningen). Ur ett operationellt perspektiv kan emellertid Prümbeslutet vara att föredra när det gäller att utbyta DNA-profiler och fingeravtrycksdata, eftersom system med indikation av ”träff” respektive ”ingen träff” garanterar direkta svar och dess modell för automatiskt utbyte av uppgifter garanterar en hög datasäkerhet.[82] På samma sätt kan det vara effektivare för finansiella underrättelseenheter, kontor för indrivning av tillgångar och plattformar för bekämpning av IT-brottslighet att kontakta sina motsvarigheter i EU direkt, utan att fylla i de formulär som krävs för att begära uppgifter inom ramen för det svenska initiativet.

Kontrollerade åtkomsträttigheter

Tillgången till system som skapats som ett led i kampen mot terrorism och allvarlig brottslighet tenderar att vara begränsad till brottsbekämpande krafter i snäv bemärkelse, det vill säga polis, gränskontroll och tullmyndigheter. Tillgång till åtgärder som skapats inom

[82] Till Prümbeslutet (rådets beslut 2008/615/RIF, EUT L 210, 6.8.2008, s. 1) finns ett motsvarande genomförandebeslut (rådets beslut 2008/616/RIF, EUT L 210, 6.8.2008, s. 12) som syftar till att garantera användningen av de senaste tekniska åtgärderna för att uppnå dataskydd och datasäkerhet och krypterings- och autentiseringsmetoder för åtkomst till uppgifterna och innhehåller specifika regler som ser till att sökningarna är tillåtna.

ramen för Schengensamarbetet beviljas typiskt sett invandringsmyndigheter och, på vissa villkor, polisen, gränskontrollen och tullmyndigheterna. Informationsflödet kontrolleras för SIS och VIS vidkommande av nationella gränssnitt. I fråga om decentraliserade system, såsom Prümbeslutet, det svenska initiativet, Neapel II-konventionen, Ecris, TFTP, PNR-avtalen, de finansiella underrättelseenheterna, kontoren för indrivning av tillgångar och plattformar för bekämpning av IT-brottslighet, sköts denna kontroll av nationella kontaktpunkter eller centrala samordningsenheter .

Olika bestämmelser om lagring av uppgifter

De perioder som uppgifter får lagras skiftar avsevärt beroende på syftena med de olika instrumenten. PNR-avtalet med Förenta staterna föreskriver den längsta lagringsperioden — 15 år, medan API har den kortaste — 24 timmar. I PNR-avtalen införs en intressant distinktion mellan uppgifter som används aktivt respektive passivt. Efter en viss period måste uppgifterna arkiveras och kan därefter endast kommas åt efter särskilt tillstånd. Kanadas användning av PNR-uppgifter från EU erbjuder ett bra exempel: information måste anonymiseras efter 72 timmar, men förblir tillgänglig för bemyndigade personer i 3,5 år.

Effektiv identitetsförvaltning

Flera av de åtgärder som analyseras ovan, inklusive det framtida SIS II och VIS, syftar till att möjliggöra identitetskontroll med hjälp av biometriska uppgifter. Genomförandet av SIS II förväntas stärka säkerheten inom området med frihet, säkerhet och rättvisa genom att bidra exempelvis till identifieringen av individer för vilka en europeisk arrestteringsorder har utfärdats, personer som har vägrats inresa i Schengenområdet och personer som söks av andra särskilda utredningsskäl (till exempel saknade personer eller vittnen i brottmål), oavsett tillgång till autentiska ID-handlingar. Genomförandet av VIS torde underlätta utfärdandet och hanteringen av viseringar.

Datasäkerhet genom EU-lösningar

För utbytet av känslig information över de europeiska gränserna föredrar medlemsstaterna att förlita sig till lösningar på EU-nivå. Flera instrument med varierande omfattning, struktur och ändamål drivs via det kommissionsfinansierade datakommunikationsnätverket s-Testa för utbyte av känsliga uppgifter. Till dessa hör de centraliserade systemen SIS II, VIS och Eurodac, men även decentraliserade instrument såsom Prümbeslutet, Ecris och de finansiella underrättelseenheterna, samt Europol och Eurojust. CIS och FIDE använder det gemensamma kommunikationsnät, det gemensamma systemgränssnitt eller den säkra webbaccess som tillhandahålls av kommissionen. Samtidigt tycks Europols nätverk för informationsutbyte Siena ha blivit det alternativ som föredras av vissa nya initiativ som förlitar sig till säker dataöverföring. Diskussioner pågår om huruvida man bör driva de finansiella underrättelseenheterna, kontoren för indrivning av tillgångar och plattformarna för bekämpning av IT-brottslighet på grundval av denna applikation.

Skiftande tillsynsmekanismer

De instrument som analyserats ovan omfattar en rad olika tillsynsmekanismer. När det gäller komplexa informationssystem såsom SIS II, VIS och Eurodac, är kommissionen skyldig att årligen eller vart annat år lägga fram rapporter om funktionen hos eller genomförandeläget för dessa system. Ett decentraliserat informationsutbyte kräver att kommissionen några år efter genomförandet lägger fram en enda utvärderingsrapport för de andra institutionerna:

direktivet om lagring av uppgifter, det svenska initiativet och åtgärderna rörande kontoren för indrivning av tillgångar ska utvärderas 2010, Prümbeslutet 2012 och Ecris 2016. I de tre PNR-avtalen finns bestämmelser om såväl regelbunden som särskild översyn, och två av dem innehåller också tidsfristklausuler. Europol och Eurojust lägger fram årliga rapporter för rådet, som vidarebefordrar dem för kännedom till Europaparlamentet. Dessa överväganden antyder att den nuvarande strukturen för informationshantering i EU inte befrämjar införandet av en gemensam utvärderingsmekanism för alla instrumenten. Sett till till denna spridning är det av största betydelse att framtida ändringar av instrument som rör informationshantering utformas med hänsyn till deras potentiella inverkan på alla andra åtgärder som reglerar insamling, lagring eller utbyte av personuppgifter inom området med frihet, säkerhet och rättvisa.

4. PRINCIPER FÖR UTVECKLINGEN AV STRATEGIER

I avsnitt 2 beskrevs flera initiativ som Europeiska kommissionen har genomfört, lagt fram eller övervägt under senare år. Enbart antalet nya idéer och den växande massan av lagstiftning när det gäller inre säkerhet och migrationshantering gör det nödvändigt att fastställa en ny uppsättning centrala principer som ska fungera som riktmärke för utarbetandet och utvärderingen av förslag till strategier under kommande år. Dessa principer bygger på, och syftar till att komplettera, de allmänna principer som följer av EU-fördragen, EU-domstolens och Europadomstolens för de mänskliga rättigheterna rättspraxis samt relevanta interinstitutionella avtal mellan Europaparlamentet, rådet och Europeiska kommissionen. Kommissionen föreslår att nya initiativ utformas och genomförs och att befintliga instrument utvärderas på grundval av följande två uppsättningar av principer:

Materiella principer

Tillvarata grundläggande rättigheter, särskilt rätten till integritets- och uppgiftsskydd

Skyddet av människors grundläggande rättigheter, såsom de kommer till uttryck i Europeiska unionens stadga om de grundläggande rättigheterna, särskilt deras rätt till integritets- och uppgiftsskydd, kommer att vara en mycket viktig aspekt för kommissionen att ta hänsyn till vid utarbetandet av nya förslag som rör behandling av personuppgifter på området för inre säkerhet och migrationshantering. I artiklarna 7 respektive 8 i stadgan uttrycks vars och ens rätt till ”respekt för sitt privatliv och familjeliv” och ”skydd av de personuppgifter som rör honom eller henne”.[83] I artikel 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), som bindande med avseende på åtgärder som vidtas av medlemsstaterna och EU:s institutioner, byråer och organ, bekräftas vars och ens rätt till ”skydd av de personuppgifter som rör honom eller henne”.[84] Vid utarbetandet av nya instrument som förutsätter användning av informationsteknik kommer kommissionen att sträva efter att följa en strategi som bygger på inbyggda säkerhets mekanismer (*privacy by design*). Detta innebär att ett skydd för personuppgifter byggs in i den tekniska basen för ett föreslaget. Behandlingen av uppgifter inskränks då till vad som är nödvändigt för att nå ett visst ändamål och tillgången till uppgifterna begränsas till de enheter som verkligen behöver dem (*need to know*)”.[85]

---

83 Europeiska unionens stadga om de grundläggande rättigheterna, EUT C 83, 30.3.2010, s. 389.

84 Konsoliderade versioner av fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, EUT C 83, 30.3.2010.2008, s. 1.

85 För en heltäckande beskrivning av inbyggda skyddsmekanismer för att skydda den personliga integriteten, hänvisas till Europeiska datatillsynsmannens yttrande om att öka förtroendet i

Nödvändighet

Inskränkningar i den enskildes rätt till respekt för privatlivet från en offentlig myndighets sida kan vara ett nödvändigt ont med hänsyn till den nationella säkerheten, den allmänna säkerheten eller förebyggandet av brott.[86] Genom Europadomstolens rättspraxis fastslås tre förutsättningar som ska vara för handen för att sådana inskränkningar ska kunna komma i fråga: ingreppet ska vara lagligt, syfta till att uppfylla ett legitimt ändamål och vara nödvändigt i ett demokratiskt samhälle. Ett ingrepp i rätten till respekt för privatlivet anses nödvändigt om det är ett svar på ett trängande samhällsbehov, om det är proprtionerligt i förhållande till det mål som ska uppnås och om de skäl som den offentliga myndigheten anför för att motivera åtgärden är relevanta och tillräckliga.[87] I alla framtida strategiska upplägg kommer kommissionen att göra en bedömning av initiativets förväntade inverkan på den enskildes rätt till respekt för privatlivet och skydd av personuppgifter, och ange varför en sådan inverkan är nödvändig och varför den föreslagna lösningen är proportionerlig i förhållande till det legitima ändamålet att upprätthålla den inre säkerheten i Europeiska unionen, förebygga brott eler hantera migration. Efterlevnaden av bestämmelserna om skydd av personuppgifter kommer under alla förhållanden att blir föremål för kontroll av en oberoende myndighet på nationell nivå eller EU-nivå.

Subsidiaritet

Kommissionen kommer att sträva efter att motivera sina nya förslag med hänsyn till subsidiaritets- och proportionalitetsprinciperna, i enlighet med artikel artikel 5 i protokoll nr 2 till fördraget om Europeiska unionen. Varje nytt lagförslag kommer att innehålla ett uttalande som gör det möjligt att bedöma efterlevnaden av subsidiaritetsprincipen, som fastställs i artikel 5 i fördraget om Europeiska unionen. Detta uttalande kommer att omfatta en bedömning av förslagets finansiella, ekonomiska och sociala verkningar och, i fråga om direktiv, dess betydelse med avseende på de bestämmelser som ska införas av medlemsstaterna.[88] Skälen för att anse att ett EU-mål kan uppnås bättre på EU-nivå kommer att underbyggas med kvalitativa indikatorer. Förslag till lagstiftning kommer att ta hänsyn till behovet av minimera eventuella extra bördor som drabbar EU, nationella förvaltningar, regionala myndigheter, ekonomiska operatörer och medborgare, och se till att de står i proportion till det mål som ska uppnås. När det gäller förslag om nya internationella avtal kommer uttalandet att ta upp förslagets förväntade inverkan på förbindelserna med tredjelandet i fråga.

Adekvat riskhantering

Syftet med att utbyta information inom området med frihet, säkerhet och rättvisa är ofta att analysera säkerhetshot, identifiera tendenser i den kriminella aktiviteten eller bedöma risker

---

informationssamhället genom att främja dataskydd och privatliv, Europeiska datatillsynsmannen, 18.3.2010.

86 Se artikel 8 i Europeiska konventionen om skydd av de mänskliga rättigheterna och de grundläggande friheterna (ETS No 5), Europarådet, 4.11.1950.

87 Se *Marper mot Förenade kungariket*, Europadomstolens för de mänskliga rättigheterna avgörande, Strasbourg, 4.12.2008.

88 De grundläggande principerna för konsekvensanalyser anges i Europeiska kommissionens riktlinjer för konsekvensbedömningar (SEK(2009) 92, 15.1.2009).

inom angränsande politikområden.[89] Risken är ofta, om än inte alltid, kopplad till individer vars tidigare beteende eller beteendemönster indikerar fortsatt risk i framtiden. Riskbedömningen bör emellertid grunda sig på bevis och inte på hypoteser. Nödvändighetstester och ändamålsbegränsning är av största betydelse för varje åtgärd som rör informationshantering. Utarbetandet av riskprofiler — som inte får förväxlas med profilering på grund av ras eller annan diskriminerande profilering som är oförenlig med de grundläggande rättigheterna — är ett viktigt inslag. Sådana profiler kan bidra till att fokusera resurserna på specifika individer i syfte att identifiera säkerhetshot och skydda brottsoffer.

Förfarandeorienterade principer[90]

Kostnadseffektivitet

Offentliga tjänster baserade på informationsteknik bör göra det möjligt att tillhandahålla bättre tjänster och skapa ett mervärde för skattebetalarna. Mot bakgrund av det rådande ekonomiska klimatet kommer ambitionen att vara att alla nya förslag, särskilt de som rör inrättande eller uppgradering av informationssystem, ska vara så kostnadseffektiva som möjligt. En sådan strategi kommer att ta hänsyn till redan befintliga lösningr för att minimera överlappning och maximera möjliga synergier. Kommissionen kommer att bedöma huruvida det är möjligt att nå målen med ett förslag genom en effektivare användning av befintliga instrument. Den kommer också att överväga komplettera befintliga informationssystem med hjälpfunktioner innan förslag om nya system läggs fram.

Utformning av strategier från ett ”bottom-upp"-perspektiv

Vid utarbetandet av nya initiativ är det viktigt att i ett så tidigt skede som möjligt ta fasta på återkopplingen från alla berörda aktörer, inklusive nationella myndigheter med ansvar för genomförandet, ekonomiska aktörer och det civila samhället. Utformning av nya strategier som tar hänsyn till slutanvändarnas intressen kräver horisontellt tänkande och vidsträckta samråd.[91] Därför kommer kommissionen försöka att skapa en permanent förbindelse med tjänstemän och rättstillämpare genom rådets strukturer, förvaltningskommittéer och tillfälligt sammansatta grupper.

En tydlig ansvarsfördelning

Sett till de tekniska komplikationer som är förknippade med projekt som rör insamling och utbyte av information inom området med frihet, säkerhet och rättvisa är det viktigt att ägna särskilt uppmärksamhet åt den ursprungliga utformningen av förvaltningsstrukturer. Erfarenheterna från SIS II-projektet visar att om man misslyckas med att i ett tidigt skede definiera tydliga och stabila överbryggande mål, roller och ansvarsområden, kan detta leda till betydande merkostnader och förseningar i genomförandet. En tidig utvärdering av erfarenheterna från genomförandet av Prümbeslutet antyder att en decentraliserad förvaltningsstruktur inte heller är någon patentlösning, eftersom medlemsstaterna inte har

---

89 Praktiska exempel på lyckad riskhantering inbegriper att förhindra en utvisad person som begått grova brott i en medlemsstat att på nytt resa in i Schengenområdet via en annan medlemsstat (SIS) eller förhindra en person att ansöka om asyl i flera medlemsstater (Eurodac).

90 Dessa principer bygger på rådets slutsatser om en informationshanteringsstrategi för EU:s inre säkerhet, rådet (rättsliga och inrikes frågor), 30.11.2009.

91 De allmänna principerna för miniminormerna för offentliga samråd anges i KOM(2002) 704, 11.12.2002.

någon projektledare att vända sig till för råd om finansiella eller tekniska aspekter av genomförandet. Den framtida IT-byrån kommer eventuellt att kunna tillhandahålla sådan tekniskt rådgivning till ansvariga för informationssystem inom området med frihet, säkerhet och rättvisa. Den kan också erbjuda en plattform för olika former av medverkan från de berörda aktörernas sida i den operativa förvaltningen och i utvecklingen av IT-system. Som ett möjligt skydd mot merkostnader och förseningar till följd av förändrade krav kommer eventuella nya informationsystem inom området för frihet, säkerhet och rättvisa inte att utvecklas förrän de underliggande rättsliga instrument som fastställer systemets syfte, räckvidd och funktioner samt de tekniska detaljerna har antagits slutligt. Detta gäller särskilt när det är fråga om storskaliga IT-system.

Bestämmelser om översyn och tidsfristklausuler

Kommissionen kommer att utvärdera vart och ett av de instrument som omfattas av detta meddelande. Utvärderingen kommer att göras mot bakgrund av hela den rad av instrument som finns på området för informationshantering. Detta bör ge en tillförlitlig bild av hur enskilda instrument passar in i ett bredare perspektiv när det gäller inre säkerhet och migrationshantering. Framtida förslag kommer i lämpliga fall att omfatta en skyldighet att avge årsrapporter, regelbunden översyn och särskild översyn samt en tidsfristklausul. Befintliga instrument kommer endast att behållas om de fortsätter att tjäna det legitima syfte för vilket de utformades. I bilaga II anges översynsdatum och översynsmekanismer för vart och ett av instrumenten som omfattas av detta meddelande.

5. PERSPEKTIV

I detta meddelande ges, för första gången, en tydlig och övergripande sammanställning av EU-åtgärder som har genomförts, håller på att genomföras eller är under övervägande på områdena insamling, lagring eller gränsöverskridande utbyte av personuppgifter för ändamål som rör brottsbekämpning eller migrationshantering.

Meddelandet erbjuder medborgarna en överblick av vilka uppgifter om dem som samlas in, lagras eller utbyts, samt för vilka ändamål och av vem uppgifterna behandlas på detta sätt. Det är ett lättbegripligt referensverktyg för berörda aktörer som vill ta del i debatten om den framtida inriktningen på EU:s politik inom detta område. Samtidigt är det ett första svar på Europeiska rådets uppmaning att utveckla instrument för informationshantering på EU-nivå i enlighet med EU-strategin för informationshantering[92] och att överväga behovet av en europeisk modell för informationsutbyte.[93]

Kommissionen har för avsikt att följa upp detta meddelande genom att lägga fram ett meddelande om en europeisk modell för informationsutbyte 2012.[94] Därför inledde kommissionen i januari 2010 en genomgång (*information mapping*) av de rättsliga grunderna för medlemsstaternas utbyte av underrättelser och information om brottlighet och av hur detta

---

92 Rådets slutsatser om en informationshanteringsstrategi för EU:s inre säkerhet, rådet (rättsliga och inrikes frågor), 30.11.2009 (EU:s informationshanteringsstrategi).

93 Stockholmsprogrammet — Ett öppet och säkert Europa i medborgarnas tjänst och för deras skydd, Rådsdokument 5731/10, 3.3.2010, avsnitt 4.2.2.

94 Detta anges i Stockholmprogrammets handlingsplan (KOM(2010) 171, 20.4.2010).

utbyte fungerar praktiskt. Kommissionen kommer att lägga fram resultaten av denna analys för rådet och Europaparlamentet 2011.[95]

Slutligen tar detta meddelande, också för första gången, upp kommissionens syn på de breda principer som den avser att följa i det framtida utarbetandet av instrument för insamling, lagring och utbyte av uppgifter. Dessa principer kommer också att ligga till grund för utvärderingen av befintliga instrument. Genom att låta utvecklingen och utvärderingen av strategier vila på dessa principer förväntar vi oss kunna skapa större konsekvens och effektivitet i tillämpningen av befintliga och framtida instrument, på ett sätt som fullt ut rspekterar människors grundläggande rättigheter.

[95] Denna kartläggning av vem som informerar om vad och till vem urförs i nära samarbete med en projektgrupp för kartläggning av informationsflöden som består av företrädare från EU- och Efta-medlemsstaterna, Europol, Eurojust, Frontex och Europeiska datatillsynsmannen.

BILAGA I

Följande uppgifter och exempel syftar till att illustrera hur de informationshanteringsåtgärder som för närvarande tillämpas fungerar i praktiken.

Schengens informationssystem (SIS)

Totalt antal SIS-registreringar i den centrala SIS-databasen (C.SIS)[96]			
Typ av registreringar	**2007**	**2008**	**2009**
Sedlar	177 327	168 982	134 255
Tomma dokument	390 306	360 349	341 675
Skjutvapen	314 897	332 028	348 353
Utfärdade dokument	17 876 227	22 216 158	25 685 572
Fordon	3 012 856	3 618 199	3 889 098
Efterlysta personer (med alias)	299 473	296 815	290 452
Efterlysta personer (huvudnamn)	859 300	927 318	929 546
Varav:			
Personer som har efterlysts för förvarstagande för utlämning	19 119	24 560	28 666
Tredjelandsmedborgare som nekas inresa	696 419	746 994	736 868
Försvunna vuxna personer	24 594	23 931	26 707
Försvunna underåriga personer	22 907	24 628	25 612
Vittnen eller personer som omfattas av kallelse till rättegång	64 684	72 958	78 869
Personer som omfattas av särskild övervakning för att förebygga hot mot den allmänna säkerheten	31 568	34 149	32 571
Personer som omfattas av särskild övervakning för att förebygga hot mot den nationella säkerheten	9	98	253
Totalt	**22 933 370**	**27 919 849**	**31 618 951**

[96] Rådsdokument 6162/10 5.2.2010 rådsdokument 5764/09 28.1.2009 rådsdokument 5441/08 30.1.2008.

Eurodac – Rörlighet för asylsökande som lämnat nya ansökningar i samma medlemsstat eller andra medlemsstater (2008)

Medlemsstater som sänder fingeravtryck för jämförelse och får träffar från de medlemsstater (kolumnerna) där en person tidigare ansökt om asyl	Medlemsstat där den första asylansökan lämnades[97]																													Totalt antal an ansökninga	
	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	Träffar i hemlandet	To ant trä
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 6**
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 1**
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 7**
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 3**
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 7**
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**	**151**
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 4**
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 7**
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 2**
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 0**
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 0**
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 7**
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 8**
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 6**
Totalt antal första ansökningar	**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**

[97] KOM(2009) 494 25.9.2009. Träffar i hemlandet avser lämnandet av en ny asylansökan i den medlemsstat där den tidigare ansökan lämnades.

Systemet för förhandsinformation om passagerare (API)

Förenade kungarikets användning av förhandsinformation om passagerare för att förbättra gränskontrollerna och bekämpa illegal migration[98]	
Antal åtgärder som vidtagits under 2009	
Tidigare negativ historia (person som nekats inresa)	379
Förlorade, stulna eller annullerade pass (beslagtaget dokument)	56

[98] Den brittiska gränsförvaltningen har lämnat dessa uppgifter till kommissionen för detta meddelande.

Tullinformationssystemet (TIS)

Totalt antal ärenden som förts in i TIS-databasen (2009)[99]	
Åtgärd	**TIS (bygger på TIS-konventionen)**
Registrerade utredningar	2 007
Pågående utredningar	274
Utredningar där frågor ställs	11 920
Raderade utredningar	1 355

[99] Dessa uppgifter har lämnats av kommissionen.

Svenskt initiativ

Exempel på hur det svenska initiativet används för att utreda brott[100]	
Dråp	Under 2009 gjordes ett försök till dråp i en medlemsstats huvudstad. Polisen tog ett biologiskt prov från ett glas som den misstänkte hade druckit ur. Genom att extrahera DNA från provet kunde kriminalteknikerna ta fram en DNA-profil. Ingen träff gavs när denna profil jämfördes med andra referensprofiler i den nationella DNA-databasen. Den utredande poliskåren sände därför, via sin Prümkontaktpunkt, en begäran om jämförelse av denna DNA-referensprofil med profiler i andra medlemsstater, vilka fått tillåtelse att utbyta sådana uppgifter på grundval av Prümbeslutet eller Prümavtalet. Denna gränsöverskridande jämförelse gav en träff. På grundval av det svenska initiativet begärde den utredande poliskåren ytterligare uppgifter om den misstänkte. Inom 36 timmar mottog polisens nationella kontaktpunkt svar från flera andra medlemsstater, vilket ledde till att polisen kunde identifiera den misstänkte.
Våldtäkt	Under 2003 våldtogs en kvinna av en oidentifierad person. Polisen tog prover från offret, men den DNA-profil som togs fram från proverna matchade inte någon referensprofil i den nationella DNA-databasen. Man fick en träff när man begärde att jämförelser av DNA skulle göras. Prüms kontaktpunkt sände begäran till andra medlemsstater, vilka getts tillåtelse att utbyta DNA-referensprofiler på grundval av Prümbeslutet eller Prümavtalet. Jämförelsen gav en träff. Den utredande poliskåren begärde därefter ytterligare uppgifter om den misstänkte på grundval av det svenska initiativet. Inom åtta timmar mottog polisens nationella kontaktpunkt ett svar, vilket gjorde det möjligt för polisen att identifiera den misstänkte.

[100] En medlemsstats poliskår lämnade dessa exempel till kommissionen för detta meddelande.

Tysklands träffar vid gränsöverskridande jämförelser av DNA-profiler efter typ av brott (2009)[101]

Träffar per typ av brott	Österrike	Spanien	Luxemburg	Nederländerna	Slovenien
Brott mot allmänna intressen	32	4	0	5	2
Brott mot personlig frihet	9	3	5	2	0
Sexualbrott	40	22	0	31	4
Brott mot person	49	24	0	15	2
Andra brott	3 005	712	18	1 105	71

[101] Tyska regeringens svar på frågor från parlamentsledamöterna Ulla Jelpke Inge Höger och Jan Korte (referensnr. 16/14120) Bundestag 16:e plenarsammanträdet referensnr. 16/14150 22.10.2009. Dessa uppgifter avser den period som började med att en medlemsstat inledde uppgiftsutbyte med Tyskland och avslutades den 30 september 2009.

Exempel på medlemsstater som upptäcker fall av allvarlig brottslighet genom lagring av uppgifter[102]	
Mord	En medlemsstats polismyndighet spårade upp en grupp mördare ansvariga för att av rasistiska skäl ha dödat sex personer. Gärningsmännen försökte undgå att infångas genom att ändra sina SIM-kort, men de avslöjades genom sina samtalslistor och IMEI-koder.
Dråp	En polismyndighet lyckades bevisa att två misstänka var inblandade i ett dråp genom att analysera trafikuppgifter från offrets mobiltelefon. Det gjorde det möjligt för poliserna att rekonstruera den väg som offret och de två misstänkta hade rest tillsammans.
Stöld	Polismyndigheterna lyckades spåra upp en gärningsman ansvarig för 17 stölder genom att undersöka trafikuppgifter från hans anonyma förbetalda SIM-kort. Genom att identifiera hans flickvän kunde de också lokalisera gärningsmannen.
Bedrägeri	Utredande poliser avslöjade en bluff där ett gäng som annonserade om kontantförsäljning av dyra bilar på internet systematiskt rånade de personer som dök upp för att ta de köpta fordonen i besittning. En IP-adress gjorde det möjligt för polisen att spåra upp annonsören och gripa gärningsmännen.

[102] Dessa anonyma exempel baseras på medlemsstaternas svar på ett av kommissionens frågeformulär från 2009 avseende införlivandet av direktiv 2006/24/EG (direktivet om lagring av uppgifter).

Samarbete mellan finansiella underrättelsetjänster (FIU)

Totalt antal begäran om uppgifter från nationella FIU via FIU.net[103]		
År	**Begäran om uppgifter**	**Aktiva användare**
2007	3 133	12 medlemsstater
2008	3 084	13 medlemsstater
2009	3 520	18 medlemsstater

[103] FIU.nets kontor har lämnat dessa uppgifter till kommissionen för detta meddelande.

Samarbete mellan kontor för återvinning av tillgångar

Medlemsstaternas begäran om spårande av tillgångar som behandlas av Europol[104]

År	**2004**	**2005**	**2006**	**2007**
Begäran	5	57	53	133
Varav:				
Ärenden som rör bedrägeri				29
Ärenden som rör penningtvätt				26
Ärenden som rör narkotika				25
Ärenden som rör andra brott				18
Ärenden som rör narkotika och penningtvätt				19
Ärenden som rör bedrägeri och penningtvätt				7
Ärenden som rör en blandning av brott				9

Ärenden som rör förverkande av tillgångar som behandlas av Eurojust (2006–2007)[105]

Typ av ärende		**Ärenden inledda av**	
Ärenden som rör miljöbrott	1	Tyskland	27%
Ärenden som rör deltagande i en kriminell organisation	5	Nederländerna	21%
Ärenden som rör narkotikahandel	15	Förenade kungariket	15%
Ärenden som rör skattebedrägeri	8	Finland	13%
Ärenden som rör bedrägeri	8	Frankrike	8%
Ärenden som rör momsbedrägeri	1	Spanien	6%
Ärenden som rör penningtvätt	9	Portugal	4%
Ärenden som rör korruption	1	Sverige	2%
Ärenden som rör brott mot egendom	2	Danmark	2%
Ärenden som rör handel med vapen	1	Lettland	2%
Ärenden som rör varumärkesförfalskning och piratkopiering	2		
Ärenden som rör bedrägeri genom förskottsavgifter	2		
Ärenden som rör förfalskning av administrativa handlingar	1		
Ärenden som rör fordonsbrottslighet	1		
Ärenden som rör terrorism	1		
Ärenden som rör förfalskning	2		

[104] Bedömning av EU-medlemsstaternas effektivitet vad gäller identifiering spårande frysning och förverkande av tillgångar som härrör från brottslig verksamhet – Slutlig rapport (för Europeiska kommissionen GD JLS) Matrix Insight 6.2009.

[105] Ibid.

Ärenden som rör människohandel	1

Plattformar mot cyberbrottslighet

Exempel från den franska plattformen mot cyberbrottslighet, Pharos som undersöker ärenden som rör it-brottslighet[106]	
Barnpornografi	En internetanvändare rapporterade om förekomsten av en blogg som innehöll foton och tecknade bilder av sexuella övergrepp mot barn till Pharos. Bloggens upphovsman som uppträdde naken på ett foto, undervisade också barn på sin blogg. Polisen identifierade en matematiklärare som huvudmisstänkt. Vid en genomsökning av hans hem upptäckts 49 videofilmer som innehöll barnpornografiska bilder. Undersökningen visade också att han förberedde en kurs för hemundervisning. Svaranden blev senare dömd och fick villkorligt fängelsestraff.
Sexuella övergrepp mot barn	Den franska polisen fick tips om en person som erbjöd pengar via Internet för sex med barn. En kriminalpolis från Pharos som uppgav sig vara underårig tog kontakt med den misstänkte, som erbjöd honom pengar för sex. Den chat som följde på Internet gjorde det möjligt att identifiera den misstänktes IP-adress och därigenom spårades han till en stad som är känd för sitt höga antal fall av sexuella övergrepp mot barn. Svaranden blev senare dömd och fick villkorligt fängelsestraff.

[106] Pharos är en förkortning av *plate-forme d'harmonisation d'analyse de recoupement et d'orientation des signalements*.

Exempel på Europols bidrag till kampen mot allvarliga gränsöverskridande brott[107]	
Operation Andromeda	I december 2009 hjälpte Europol till att genomföra en stor gränsöverskridande polisinsats mot ett narkotikahandelsnätverk med kontakter i 42 länder. Nätverket hade sin bas i Belgien och Norge och sålde narkotika från Peru via Nederländerna till Belgien, Förenade kungariket, Italien och andra medlemsstater. Europol samordnade polissamarbetet och Eurojust samordnade det rättsliga samarbetet. De myndigheter som deltog inrättade ett mobilt kontor i Pisa och Europol och hade en ledningscentral i Haag. Europol gjorde korsreferenser av uppgifterna mellan de misstänka och utarbetade en rapport som skildrade det kriminella nätverket.
Deltagare	Italien, Nederländerna, Tyskland, Belgien, Förenade kungariket, Litauen, Norge och Eurojust.
Resultat	De deltagande polismyndigheterna beslagtog 49 kg kokain, 10 kg heroin, 6 000 ecstasypiller, två skjutvapen, fem falska identitetshandlingar och 43 000 euro i likvida medel och grep 15 personer.
Operation Typhon	Mellan april 2008 och februari 2010 gav Europol analytiskt stöd till polisstyrkor från 20 länder, som var inblandade i Operation Typhon. I denna stora insats mot ett pedofilnätverk som distribuerade barnpornografibilder via en österrikisk webbplats gav Europol tekniskt stöd och kriminalunderrättelser på grundval av de bilder som mottogs från Österrike. Europol bedömde sedan uppgifternas tillförlitlighet och omstrukturerade dem innan den utarbetade sitt eget underrättelsematerial. Genom korsreferenser av uppgifterna med dem i dess arbetsregister för analysändamål kunde Europol utarbeta 30 underrättelserapporter som gav upphov till utredningar i flera länder.
Deltagare	Österrike, Belgien, Bulgarien, Kanada, Danmark, Frankrike, Tyskland, Ungern, Italien, Litauen, Luxemburg, Malta, Nederländerna, Polen, Rumänien, Slovakien, Slovenien, Spanien, Schweiz och Förenade kungariket.
Resultat	I detta ärende identifierade de deltagande myndigheterna 286 misstänkta, grep 118 misstänkta och undsatte fem offer i fyra länder som utsatts för övergrepp.

[107] Europol har lämnat dessa uppgifter till kommissionen för detta meddelande. Närmare upplysningar om Operation Andromeda finns på http://www.eurojust.europa.eu/.

Eurojust

Exempel på hur Eurojust samordnat stora gränsöverskridande rättsliga åtgärder mot allvarlig brottslighet[108]	
Människohandel och finansiering av terrorism	I maj 2010 samordnade Eurojust en gränsöverskridande insats som resulterade i gripandet av fem medlemmar i ett organiserat brottsligt nätverk aktivt i Afghanistan, Pakistan, Rumänien, Albanien och Italien. Gruppen försåg medborgare från Afghanistan och Pakistan med förfalskade handlingar och smugglade dem till Italien via Iran, Turkiet och Grekland. Vid ankomsten till Italien sändes migranterna till Tyskland, Sverige, Belgien, Förenade kungariket och Norge. Vinsterna från människohandeln var avsedd att finansiera terrorism.
Bankkortsbedrägeri	Genom att samordna gränsöverskridande polissamarbete och rättsligt samarbete hjälpte Europol och Eurojust till att reda ut ett bankkortsbedrägerinätverk som var aktivt i Irland, Italien, Nederländerna, Belgien och Rumänien. Nätverket stal identifikationsuppgifter från cirka 15 000 betalkort, vilket förorsakade en förlust på 6,5 miljoner euro. Före insatsen, vilken resulterade i 24 gripanden i juli 2009 underlättade domare från Belgien, Irland, Italien, Nederländerna och Rumänien utfärdandet av europeiska arresteringsorder och begäran om avlyssning av de misstänkta personerna.
Människohandel och narkotikahandel	Efter ett samordningsmöte som Eurojust organiserade i mars 2009 grep de italienska, nederländska och colombianska myndigheterna 62 personer misstänkta för människohandel och narkotikahandel. Nätverket smugglade utsatta kvinnor från Nigeria till Nederländerna och tvingade in dem i prostitution i Italien, Frankrike och Spanien. Vinsterna från prostitutionen finansierade nätverkets inköp av kokain i Colombia som sändes till EU för konsumtion.

[108] Dessa exempel härrör från http://www.eurojust.europa.eu/.

Passageraruppgifter (PNR-uppgifter):

Exempel på PNR-analys som ger information för undersökning av allvarliga gränsöverskridande brott[109]	
Handel med barn	PNR-analysen avslöjade att tre ensamkommande barn reste från en EU-medlemsstat till ett tredjeland, utan några uppgifter om vem som skulle möta dem när de anlände. Efter att medlemsstatens polismyndighet förvarnat tredjelandets myndigheter efter avresan greps den person som kom för att hämta barnen: en sexualbrottsling registrerad i medlemsstaten.
Människohandel	PNR-analys avslöjade en grupp människohandlare som alltid reste samma väg. De använde falska handlingar för att checka in på ett flyg inom EU samtidigt som de använde äkta handlingar för att checka in på en annan flygning på väg till tredjeland. Så snart de befann sig i flygplatsens lounge gick de ombord på flyget inom EU.
Kreditkortsbedrägeri	Flera familjer reste till en medlemsstat med biljetter som köpts med stulna kreditkort. Efterforskningar visade att en kriminell grupp använde dessa kort för att köpa biljetterna och sedan sälja dem över disk från långväga teletjänstcentraler. PNR-uppgifterna kopplade ihop de resande med kreditkorten och säljarna.
Narkotikahandel	En medlemsstats polismyndighet hade uppgifter som tydde på att en man var inblandad i narkotikahandel från ett tredjeland, men gränsvakterna hittade aldrig något på honom när han anlände till EU. PNR-uppgifterna visade att han alltid reste med en medarbetare. En undersökning av hans medarbetare ledde till att stora mängder narkotika hittades.

[109] Dessa exempel är anonyma för att skydda informationskällorna.

Program för att spåra finansiering av terrorism (TFTP)

Exempel på hur programmet för att spåra finansiering av terrorism gett uppgifter så att man kunnat undersöka terroristdåd[110]	
Terroristdådet i Barcelona 2008	I januari 2008 greps tio misstänkta i Barcelona i samband med ett misslyckat försök att utföra en attack på stadens kollektivtrafiksystem. Uppgifter från programmet användes för att identifiera de misstänktas kopplingar till Asien, Afrika och Nordamerika.
Transatlantiskt terrordåd med bomb på flytande vätska 2006	Uppgifter från programmet användes för att undersöka och döma personer i samband med ett misslyckat dåd i augusti 2006 avsett att spränga tio transatlantiska flyg från Förenade kungariket på väg till Förenta staterna och Kanada.
Bombattentaten i London 2005	Uppgifter från programmet användes för att ge poliserna nya ledtrådar, bekräfta de misstänktas identiteter och avslöja förbindelser mellan personerna ansvariga för denna attack.
Bombattentaten i Madrid 2004	Uppgifter från programmet lämnades till flera EU-medlemsstater för att bistå dem i deras undersökningar efter attacken.

[110] Andra rapporten om behandlingen av personuppgifter med ursprung i EU av *United Stated Treasury Department for counter-terrorism purposes*, domare Jean-Louis Bruguière, januari 2010.

BILAGA II

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Schengens informationssystem (SIS)	På initiativ av medlemsstaterna	Upprätthålla allmän säkerhet inklusive nationell säkerhet i Schengenområdet och underlätta människors rörlighet genom att använda uppgifter som meddelas via detta system.	Centraliserad: N.SIS (nationella delar) anslutet med gränssnitt till C.SIS (central del).	Namn och alias fysiska kännetecken, födelseort och födelsedatum, medborgarskap och om en person är beväpnad eller våldsbenägen. SIS-registreringarna avser flera olika grupper av personer.	Polis, gränspolis, tull och rättsliga myndigheter har tillgång till alla uppgifter. Invandrarmyndigheter och konsulära myndigheter har tillgång till förteckningar över inreseförbud och förlorade och stulna handlingar. Europol och Eurojust har tillgång till vissa uppgifter.	Europarådets konvention 108, Europaråadets polisrekommendation R (87) 15.	Personuppgifter som förs in i SIS för att spåra personer får bara behållas under den tidsperiod som krävs för att uppfylla det syfte för vilket de lämnades och högst tre år. Uppgifter om personer som omfattas av särskild övervakning till följd av det hot de utgör för den allmänna eller nationella säkerheten ska raderas efter ett år.	SIS är fullt tillämpligt i 22 medlemsstater plus Schweiz, Norge och Island. Förenade kungariket och Irland deltar i SIS, med undantag för registreringar av tredjelandsmedborgare med inreseförbud. Bulgarien, Rumänien och Liechtenstein väntas genomföra systemet inom kort.	Signatärer kan föreslå ändringar till Schengenkonventionen. Den ändrade texten ska antas med enhällighet och ratificeras av parlamenten.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Schengens informationssystem II (SIS II)	På initiativ av kommissionen	Att garantera en hög säkerhetsnivå i området med frihet säkerhet och rättvisa och underlätta människors rörlighet genom att använda uppgifter som meddelas via detta system.	Centraliserad: N.SIS (nationella delar) anslutet med gränssnitt till C.SIS (central del). SIS II körs på det säkra nätverket s-TESTA.	Uppgiftskategorier i SIS plus fingeravtryck och foton, kopior av europeiska arresteringsordern, felanvända identitetsregistreringar och kopplingar mellan registreringar. SIS II-registreringarna avser flera olika grupper av personer.	Polis, gränspolis, tull och rättsliga myndigheter kommer att ha tillgång till alla uppgifter. Invandrarmyndigheter och konsulära myndigheter har tillgång till förteckningar över inreseförbud och förlorade och stulna handlingar. Europol och Eurojust kommer att få tillgång till vissa uppgifter.	Särskilda regler som införts genom de grundläggande rättsakter som reglerar SIS II och direktiv 95/46/EG förordning (EG) 45/2001 rådets rambeslut 2008/977/RIF förordning (EG) 45/2011 Europarådets konvention 108 och Europarådets polisrekommendation R (87) 15.	Personuppgifter som förs in i SIS för att spåra personer får bara behållas under den tidsperiod som krävs för att uppfylla det syfte för vilket de lämnades och högst tre år. Uppgifter om personer som omfattas av särskild övervakning till följd av det hot de utgör för den allmänna eller nationella säkerheten ska raderas efter ett år.	SIS II håller på att genomföras. Så snart det genomförts kommer det att tillämpas i EU-27 Schweiz, Liechtenstein Norge och Island. Förenade kungariket och Irland kommer att delta i SIS II, med undantag för registreringar av tredjelandsmedborgare med inreseförbud.	Kommission måste sända halvårsvisa lägesrapporter till Europaparlamentet och rådet om utvecklingen av SIS II och dess eventuella migration från SIS.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Eurodac	På initiativ av kommissionen	Bidra till att fastställa vilken medlemsstat som ska utvärdera asylansökan.	Centraliserad, bestående av nationella anslutningspunkter, anslutet med gränssnitt till Eurodacs centrala enhet. Eurodac körs på nätverket s-TESTA.	Uppgifter om fingeravtryck, kön, ort och datum där asylansökan lämnades, referensnummer som används av den ursprungliga medlemsstaten och datum då fingeravtryck togs, överfördes och fördes in i systemet.	Medlemsstaterna ska specificera vilka myndigheter som har tillgång till uppgifterna vilka normalt inkluderar asyl- och migrationsmyndigheter gränsvakter och polis.	Direktiv 95/46/EG.	Tio år för asylsökandens fingeravtryck. Två år för fingeravtryck från medborgare i tredjeländer som grips när de olagligen passerar en yttre gräns.	Eurodac-förordningen gäller i var och en av medlemsstaterna, Norge, Island och Schweiz. Ett avtal som gör det möjligt för Liechtenstein att ansluta sig håller på att avslutas.	Kommissionen ska sända en årsrapport till Europaparlamentet och rådet om användningen av Eurodacs centralenhet.
Informationssystemet för viseringar (VIS)	På intiativ av kommissionen	Bidra till att genomföra en gemensam viseringspolitik och förhindra hot mot den inre säkerheten.	Centraliserad, bestående av nationella delar som ska anslutas med gränssnitt till den centrala delen. VIS körs på nätverket s-TESTA.	Viseringansökningar fingeravtryck, foton, relaterade viseringsbeslut och kopplingar mellan relaterade program.	Viserings-, asyl-, immigrations- och gränskontroll myndigheter kommer att ha tillgång till alla uppgifter. Polis och Europol kan konsultera VIS för att förhindra upptäcka och utreda allvarliga brott.	Särskilda regler som införts genom de grundläggande rättsakter som reglerar VIS och direktiv 95/46/EG förordning (EG) 45/2001 rådets rambeslut 2008/977/RIF Europarådets konvention 108 och Europarådets polisrekommendation R (87) 15.	Fem år.	VIS håller på att genomföras och kommer att vara tillämpligt i var och en av medlemsstaterna (utom Förenade kungariket och Irland) plus Norge, Island och Schweiz.	Kommissionen ska rapportera till Europaparlamentet och rådet om driften av VIS tre år efter att det lanserats och var fjärde år därefter.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
System för förhandsinformation om passagerarna (API)	På initiativ av Spanien	Förbättra gränskontrollerna och bekämpa illegal migration.	Decentraliserad	Personuppgifter från pass, ort för ombordtigning, införselplats till EU.	Gränskontroll myndigheter och, på begäran, brottsbekämpande myndigheter.	Direktiv 95/46/EG.	Uppgifterna ska raderas 24 timmar efter det att ett flyg anlänt till EU.	API gäller i var och en av medlemsstaterna, men bara ett fåtal använder det.	Kommissionen ska utvärdera API-systemet 2011.
Neapel II-konventionen	På initiativ av medlemsstaterna	Hjälpa nationella tullmyndigheter att förhindra och upptäcka överträdelser av nationella tullbestämmelser och hjälpa dem att åtala och bestraffa överträdelser av gemenskapsbestämmelser och nationella tullbestämmelser.	Decentraliserad, drivs genom en uppsättning centrala samordningsenheter.	Alla uppgifter relaterade till en identifierad eller identifierbar person.	Centrala samordnade enheter överför uppgifter till nationella tullmyndigheter, undersökande myndigheter och rättsliga organ och vid förhandsgodkännande från de medlemsstater som lämnat uppgifterna till andra myndigheter.	Direktiv 95/46/EG och Europarådets konvention 108. Uppgifterna i den mottagande medlemsstaten ska ha en skyddsnivå som minst motsvarar nivån i den uppgiftslämnande medlemsstaten.	Uppgifterna får behållas under en tidsperiod som inte överstiger den som är nödvändig för det syfte för vilket de lämnades.	Denna konvention har ratificerats av var och en av medlemsstaterna.	Signatärer kan föreslå ändringar till Neapel II-konventionen. Den ändrade texten ska antas av rådet och ratificeras av medlemsstaterna.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Tullinformations-systemet (TIS)	På initiativ av medlemsstaterna	Bistå de behöriga myndigheterna i att förhindra, undersöka och åtala allvarliga brott mot nationella tullbestämmelser.	Centraliserad, tillgänglig via terminaler i var och en av medlemsstaterna och på kommissionen. CIS och FIDE drivs genom AFIS som använder det gemensamma kommunikationsnätet, gemensamma gränssnittet eller säker webbåtkomst från kommissionen.	Namn och alias födelsedatum och födelseort, medborgarskap, kön, fysiska egenskaper, identitetshandlingar, adress, tidigare våldsbenägenhet, orsaken till att uppgifter förs in i TIS, föreslagen åtgärd och registrering av transportmedel.	Nationella tullmyndigheter Europol och Eurojust har tillgång till uppgifterna i TIS.	Särskilda regler som införts genom TIS-konventionen och direktiv 95/46/EG, förordning (EG) nr 45/2001, Europarådets konvention 108 och Europarådets polisrekommendation R (87) 15.	Personuppgifter som kopieras från TIS till andra system för riskhantering eller driftsanalyser får bara behållas under den tidsperiod det är nödvändigt för att uppnå syftet med vilket de kopierades och högst tio år.	Gäller i var och en av medlemsstaterna.	Kommissionen i samarbete med medlemsstaterna rapporterar varje år till Europaparlamentet och rådet om driften av TIS.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Svenskt initiativ	På initiativ av Sverige.	Effektivisera informationsutbytet för brottsutredningar och kriminalunderrättelseverksamhet.	Decentraliserad meedlemsstaterna ska utse nationella kontaktpunkter som behandlar brådskande förfrågningar om information.	Eventuell befintlig information eller kriminalunderrättelse-verksamhet som finns tillgänglig för brottsbekämpande myndigheter.	Polis, tull och varje annan myndighet med befogenhet att utreda brott (med undantag av underrättelsverksamhet).	Nationella dataskyddsregler samt Europarådets konvention 108, Europarådets tilläggsprotokoll 181 och Europaraådets polisrekommendation R (87) 15.	Information och underrättelse verksamhet som lämnas genom detta instrument får bara användas för det syfte för vilket de lämnades och på de särskilda villkor som fastställts av den uppgiftslämnande medlemsstaten.	12 av de 31 signatärerna (EU-medlemsstater och Efta-stater) har antagit nationella lagar för att införa detta instrument, fem fyller i formuläret för att begära uppgifter och två använder det regelbundet för att utbyta information.	Kommissionen ska lämna sin utvärderingsrapport till rådet under 2010.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Prümbeslutet	På initiativ av medlemsstaterna	Öka förebyggandet av brott, särskilt terrorism och upprätthålla allmän ordning.	Decentraliserad, sammankopplad via nätverket s-TESTA. Nationella kontaktpunkter behandlar utgående och inkommande begäranden om jämförelse av uppgifter.	Anonyma DNA-profiler och fingeravtryck, uppgifter om fordonsregistrering och information om personer som misstänks ha kopplingar till terrorism.	Kontaktpunkterna överlämnar ansökningarna, inhemsk tillgång regleras i nationell lagstiftning.	Särskilda regler infördes genom Prümbeslutet och Europarådets konvention 108, Europarådets tilläggsprotokoll 181 och Europarådets polisrekommendation R (87) 15. Enskilda kan vända sig till sina nationella datatillsynsmän för att göra sina rättigheter gällande avseende behandlingen av personuppgifter.	Personuppgifterna ska raderas så snart de inte längre behövs för det syfte för vilket de lämnades. Den maximala inhemska datalagringsperioden för den uppgiftslämnande staten är bindande för den mottagande staten.	Prümbeslutet håller på att genomföras. Tio medlemsstater har tillåtits utbyta DNA, fem att utbyta fingeravtryck, sju att utbyta fordonsuppgifter. Norge och Island håller på att ansluta sig till detta instrument.	Kommissionen ska lämna sin utvärderingsrapport till rådet under 2012.
Direktivet om lagring av uppgifter	På initiativ av medlemsstaterna	Öka utredning, avslöjande och åtal av allvarliga brott genom att lagra telekomtrafik- och lokaliseringsuppgifter.	Decentralised, genom instrumentet införs skyldigheter för leverantörer av telekommunikationstjänster att lagra uppgifter.	Telefonnummer, IP- adress och IMEI-koder.	Myndigheter med åtkomsträtt fastställs på nationell nivå.	Direktiv 95/46/EG och direktiv 2002/58/EG.	Mellan 6 och 24 månader.	Sex medlemsstater har ännu inte infört direktivet och de tyska och rumänska författningsdomstolarna fastställde att genomförandelagstiftningen var grundlagstridig.	Kommissionen ska lämna sin utvärderingsrapport till Europaparlamentet och rådet under 2010.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris)	På initiativ av Belgien och förslag av kommissionen.	Förbättra samutnyttjande av gränsöverskridande uppgifter om brottsregister över EU-medborgare.	Decentraliserad, sammankopplat via en uppsättning centrala myndigheter som ska utbyta uppgifter som hämtats ur brottsregister genom nätverket s-TESTA.	Biografiska uppgifter, fällande dom, dömda personer och överträdelse, ytterligare uppgifter inklusive fingeravtryck (om tillgängliga).	Rättsliga och behöriga förvaltningsmyndigheter.	Särskilda regler införda genom rådets rambeslut 2009/315/RIF, som införlivar bestämmelserna i rådets beslut 2005/876/RIF, samt rådets rambeslut 2008/977/RIF, Europarådets konvention 108 och förordning (EG) nr 45/2001.	Nationella regler för datalagring gäller eftersom detta instrument bara reglerar utbyte av uppgifter.	Ecris håller på att genomföras. Nio medlemsstater har börjat utbyta uppgifter elektroniskt.	Kommissionen ska lämna två utvärderingsrapporter till Europaparlamentet och rådet om rambeslut 2008/675/RIF under 2011 och om rambeslut 2009/315/RIF under 2015. Från 2016 ska kommissionen offentliggöra regelbundna rapporter om driften av rådets beslut 2009/316/RIF (Ecris).

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Samarbete mellan finansiella underrättelsetjänster (FIU.net)	På initiativ av Nederländerna.	Utbyta uppgifter som är nödvändiga för att analysera och utreda penningtvätt och finansiering av terrorism.	Decentraliserad, finansella underrättelsetjänster utbyter uppgifter via FIU.net, som körs på nätverket s-TESTA. Europols program Siena kan snart understödja FIU.net.	Alla uppgifter av relevans för analysen eller utredningen av penningtvätt och finansiering av terrorism.	Finansiella underrättelsetjänster (inom poliskårer rättsliga myndigheter eller förvaltningsmyndigheter som rapporterar till finansiella myndigheter).	Rådets rambeslut 2008/977/RIF, Europarådets konvention 108 och Europaråadets polisrekommendation R (87) 15.	Nationella regler för datalagring gäller eftersom detta instrument bara reglerar utbyte av uppgifter.	20 medlemsstater deltar i FIU.net, ett säkert onlineprogram för samutnyttjande av uppgifter som körs på s-TESTA.	Som en del av handlingsplanen för finansiella tjänster har kommissionen sedan 2009 sett över genomförandet av direktiv 2005/60/EG.
Samarbete mellan kontor för återvinning av tillgångar (ARO)	På initiativ av medlemsstaterna	Utbyte av information som är nödvändig för att spåra och fastställa vinning av brott.	Decentraliserad, kontoren ska utbyta information via det svenska initiativet. Europols program Siena kan snart understödja samarbetet mellan kontoren.	Uppgifter om egendom som avses som bankkonton fastigheter och fordon samt uppgifter om personer som eftersöks, som namn, adress, uppgifter till aktieägare och företag.	Kontor för återvinning av tillgångar	Europarådets konvention 108, Europarådets tilläggsprotokoll 181, Europaraådets polisrekommendation R (87) 15.	Nationella regler för datalagring gäller eftersom detta instrument bara reglerar utbyte av uppgifter.	Mer än 20 medlemsstater har inrättat kontor och 12 deltar i pilotprojekt för att utveckla Europols Siena som plattform för utbyte av uppgifter av relevans för spårande av tillgångar.	Kommissionen ska lämna sin utvärderingsrapport till rådet under 2010.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Nationella plattformar och EU-plattformar mot it-brottslighet	På initiativ av Frankrike.	Insamling, utbyte och analys av uppgifter om överträdelser som har begåtts på Internet.	Decentraliserad, för samman nationella plattformar för rapportering och Europols EU-plattform mot cyberbrottslighet. Europols program Siena kan snart understödja uppgiftsutbyte mellan plattformar för rapportering.	Olagligt innehåll eller agerande som upptäckts på Internet.	Nationella plattformar som tar emot medborgarnas rapporter, Europols EU-plattform mot cyberbrottslighet tar emot meddelanden från brottsbekämpande myndigheter om allvarlig gränsöverskridande brottslighet.	Särskilda regler som införts genom Europols beslut och rådets rambeslut 2008/977/RIF, Europarådets konvention 108, Europarådets tilläggsprotokoll 181, Europarådets polisrekommendation R (87) 15 och förordning (EG) nr 45/2001.	Nationella regler för datalagring gäller eftersom detta instrument bara reglerar utbyte av uppgifter.	Nästan alla medlemsstater har inrättat nationella plattformar för rapportering. Europol arbetar med sin EU-plattform mot it-brottslighet.	Europol täcker it-brottslighet och kommer i framtiden att rapportera om sin verksamhet på EU-plattformen mot it-brottslighet i sin årsrapport som lämnas till rådet för godkännande och Europaparlamentet för information.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Europol	På initiativ av medlemsstaterna	Stödja medlemsstaterna i att förebygga och bekämpa organiserad brottslighet terrorism och andra allvarliga brott som berör två eller fler medlemsstater.	Europol är ett EU-organ med säte i Haag. Det utvecklar Siena, en nätapplikation för säkert informationsutbyte.	Europols informationssystem (EIS) innehåller personuppgifter inklusive biometriska kännetecken, fällande domar och kopplingar till organiserad brottslighet som avser personer som misstänks för brott under Europols mandat. Arbetsregistren för analysändamål innehåller alla personuppgifter av relevans.	Åtkomst till EIS ges via Europols nationella enheter, kontaktpersoner, Europols anställda och direktören. Kontaktpersonerna har åtkomst till arbetsregistren för analysändamål. Personuppgifter kan utbytas med tredjeländer som har avtal med Europol.	Särskilda regler som införts genom Europols beslut och rådets rambeslut 2008/977/RIF Europarådets konvention 108 Europarådets tilläggsprotokoll 181 Europarådets polisrekommendation R (87) 15 och förordning (EG) nr 45/2001.	Arbetsregistren för analysändamål får lagras i högst tre år med möjlighet till förlängning med ytterligare tre år.	Europol används aktivt av var och en av medlemsstaterna och tredjeländer med vilka den har ett operativt avtal. Europols nya rättsliga grund har införlivats i alla medlemsstater.	Ett gemensamt övervakningsorgan kontrollerar Europols behandling av personuppgifter och överföringen av dessa uppgifter till andra parter. Den lämnar regelbundna rapporter till Europaparlamentet och rådet. Europol lämnar också en årsrapport om sin verksamhet till rådet för godkännande och Europaparlamentet för information.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Eurojust	På initiativ av medlemsstaterna	Förbättra samordningen mellan utredningar och åtal i medlemsstaterna och öka samarbetet mellan relevanta myndigheter.	Eurojust är ett EU-organ i Haag som använder s-TESTA för utbyte av uppgifter.	Personuppgifter av misstänkta och lagbrytare i fall av allvarliga brott som berör två eller fler medlemsstater inklusive biografiska uppgifter kontaktuppgifter DNA-profiler fingeravtryck foton telekomtrafik- och lokaliseringsuppgifter.	Europols 27 nationella medlemmar kan dela uppgifter med nationella myndigheter och tredjeländer om informationskällorna samtycker.	Särskilda regler som införts genom Eurojustbeslutet och rådets rambeslut 2008/977/RIF Europarådets konvention 108, Europarådets tilläggsprotokoll 181 och Europarådets polisrekommendation R (87) 15.	Uppgifterna ska raderas så snart syftet med att tillhandahålla dem har uppfyllts och ärendet är avslutat.	Medlemsstaterna håller för närvarande på att införliva den ändrade rättsliga grunden för Eurojust.	I juni 2014 ska kommissionen se över uppgiftsutbytet mellan Eurojusts nationella medlemmar. I juni 2013 ska Eurojust till rådet och kommissionen rapportera om bestämmelsen om nationell åtkomst till dess ärende-hanteringssystem. Ett gemensamt övervakningsorgan kontrollerar Eurojusts behandling av personuppgifter och lämnar årligen rapporter till rådet. Ordföranden i Eurojustkollegiet lämnar en årsrapport till rådet om Eurojusts verksamhet, vilken rådet i sin tur för vidare till Europaparlamentet.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
Avtal om passagerar uppgifter med USA och Australien; API-/PNR-avtal med Kanada	På initiativ av kommissionen.	Förebygga och bekämpa terrorism och andra former av allvarlig gränsöverskridande brottslighet.	Internationella avtal.	Avtalen med USA och Australien innehåller 19 kategorier av passageraruppgifter inklusive biografiska uppgifter, uppgifter om reservation och betalning samt kompletterande uppgifter. Avtalet med Kanada innehåller 25 liknande uppgifter.	US Department of Homeland Security, Canada Border Services Agency och Australian Customs Service kan dela uppgifter med inhemska brottsbekämpande avdelningar och avdelningar för bekämpande av terrorism.	Reglerna för skydd av personuppgiter anges i de särskilda internationella avtalen.	USA: 7 års aktiv och 8 års passiv användning. Australien: 3,5 års aktiv och 2 års passiv användning. Kanada: 72 timmars aktiv och 3,5 års passiv användning.	Avtalen med USA och Australien är preliminärt tillämpliga. Avtalet med Kanada gäller. Kommissionen kommer att omförhandla dessa avtal. Sex medlemsstater har antagit lagar som gör det möjligt att använda passageraruppgifter i brottsbekämpande syfte.	I varje avtal föreskrivs regelbunden översyn medan avtalen med Kanada och Australien även inkluderar uppsägningsklausuler.

Översikt i tabellform av instrument som används, håller på att genomföras eller övervägas

Instrument	Bakgrund	Syfte(n)	Struktur	Täckning av personuppgifter	Åtkomst till uppgifter	Uppgiftsskydd	Datalagring	Fas i genomförandet	Översyn
TFTP-avtal mellan EU och USA	På initiativ av kommissionen.	Förhindra, utreda, avslöja eller åtala terrorism eller finansiering av terrorism.	Internationellt avtal.	Finansiella betalningsmeddelanden, som bland annat innehåller namn, kontonummer, adress och ID-nummer på beställaren och mottagaren av finansiella transaktioner.	US Treasury kan dela personuppgifter som hämtats från finansiella meddelanden med amerikanska brottsbekämpande myndigheter, myndigheter för allmän säkerhet eller terroristbekämpande myndigheter, medlemsstater, Europol eller Eurojust. Vidare överföring till tredjeländer beror på medlemsstaternas samtycke.	Ändamålet med avtalet är strikt avgränsat och det innehåller proportionalitetsklausuler.	Personuppgifter som hämtats från finansiella meddelanden får inte behållas längre än nödvändigt vid individuella utredningar eller åtal. Uppgifter som inte tagits fram får bara behållas i fem år.	Europaparlamentet gav sitt samtycke till ingående av TFTP-avtalet mellan EU och USA den 8 juli 2010. Rådet väntas nu anta ett rådsbeslut om ingående av detta avtal, varefter avtalet träder i kraft via ett utbyte av skrivelser mellan parterna.	Kommissionen ska se över avtalet sex månader efter det att det trädde i kraft. Dess utvärderingsrapport ska sändas till Europaparlamentet och rådet.