Ds 2009:8

Genomförandet av delar av Prümrådsbeslutet

REGERINGSKANSLIET
Justitiedepartementet

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 2003.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/

Tryckt av Edita Sverige AB
Stockholm 2009

ISBN 978-91-38-23168-5
ISSN 0284-6012

Till statsrådet och chefen för Justitiedepartementet

Chefen för Justitiedepartementet, statsrådet Ask, beslutade den 9 juli 2008 att uppdra åt överåklagaren Gunnel Lindberg att biträda departementet dels med genomförandet av rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (det s.k. svenska initiativet), dels med utarbetandet av en promemoria som behandlar genomförandet av de huvudsakliga delarna av rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (det s.k. Prümrådsbeslutet). Hovrättsassessorn Li Wallén har tjänstgjort som sekreterare.

I september 2008 överlämnandes promemorian *Enklare informationsutbyte i brottsbekämpningen inom EU* (Ds 2008:72).

Härmed överlämnas promemorian *Genomförandet av delar av Prümrådsbeslutet*.

Uppdraget är i och med detta i sin helhet slutfört.

Stockholm i mars 2009

Gunnel Lindberg

/Li Wallén

Innehåll

1 Promemorians huvudsakliga innehåll

Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet) syftar till att fördjupa det gränsöverskridande samarbetet mellan de myndigheter inom Europeiska unionen som ansvarar för att förebygga och utreda brott. I huvudsak ska detta ske genom förenklade former för utbyte av uppgifter om DNA-profiler, fingeravtryck och fordon.

I denna promemoria redovisas de författningsändringar som bedöms vara nödvändiga och lämpliga för att genomföra de obligatoriska delarna av Prümrådsbeslutet i svensk rätt. Avgränsningen av uppdraget framgår av *bilaga 1*.

Rådsbeslutet och därtill hörande genomförandebeslut fogas till denna promemoria i svensk översättning som *bilaga 2 och 3*.

Rådsbeslutet aktualiserar inte inrättandet av några nya databaser. Kravet på att det ska finnas nationella register med DNA-profiler är uppfyllt genom de DNA-register som Rikspolisstyrelsen för.

Redan i dag utbyts den typ av uppgifter som enligt rådsbeslutet i fortsättningen kommer att kunna inhämtas direkt genom sökningar i andra staters databaser. Den stora skillnaden i förhållande till dagens ordning blir att informationsutbytet kan ske automatiserat, på elektronisk väg, och att den som behöver informationen omedelbart kan få besked om det finns någon uppgift av intresse eller inte. De automatiska sökningar som

rådsbeslutet förutsätter ska kunna ske i andra medlemsstaters DNA-register i samband med brottsutredning kräver ny reglering. Detsamma gäller rätten att under vissa förutsättningar göra automatiska jämförelser av oidentifierade DNA-profiler. Även automatiska sökningar i fingeravtrycksregister för att förebygga eller utreda brott måste regleras. Förslagen innebär att särskilda kontaktställen i andra stater ges rätt att under vissa förhållanden genomföra sökningar i de svenska registren och att hämta information i form av referensuppgifter från dessa. Det krävs också regler som ger det svenska kontaktstället möjlighet att söka efter uppgifter i andra staters register.

Den nya lagstiftningen föreslås i huvudsak genomföras i polisdatalagen (1998:622), där DNA-register och fingeravtrycksregister regleras, och i lagen (2000:343) om internationellt polisiärt samarbete. Själva förfarandet vid utbyte av uppgifter bedöms kunna regleras i förordning. Promemorian innehåller, förutom lagförslagen, förslag till huvuddelen av de förordningsregler som krävs.

Informationsutbytet påverkar inte det grundläggande integritetsskydd vid personuppgiftsbehandling som bl.a. polisdatalagen och personuppgiftslagen ger. Vid sökningar i de svenska registren ska de mera integritetskänsliga uppgifterna, DNA-profiler och fingeravtryck, aldrig kunna hänföras till en identifierbar person. På samma sätt som i dag måste den stat som vill ha upplysning om vem uppgiften avser begära rättslig hjälp. Sådan rättslig hjälp regleras inte i rådsbeslutet. Däremot föreslås en ny bestämmelse i lagen (2000:562) om internationell rättslig hjälp i brottmål som reglerar rättslig hjälp med att samla in och analysera DNA-prov från en person som vistas här i landet samt översända den DNA-profil som fastställts genom analysen till en annan stat. Det föreslås även en särskild regel om förstörande av sådana DNA-prov.

Genom rådsbeslutet utvecklas också formerna för att utbyta vissa uppgifter om fordon. Det som omfattas är uppgifter om fordon och fordons ägare eller innehavare. För att Sverige ska kunna leva upp till kraven i rådsbeslutet föreslås bl.a. att ända-

målsbestämmelsen i lagen (2001:558) om vägtrafikregister utvidgas så att andra stater kan ges direktåtkomst till vissa uppgifter i registret för att förebygga och utreda brott, undersöka vissa överträdelser eller för att upprätthålla allmän säkerhet.

Rådsbeslutet reglerar vidare bl.a. skyldigheten att vid större evenemang med gränsöverskridande verkningar översända personuppgifter och andra uppgifter till en annan medlemsstat, om uppgifterna bedöms vara nödvändiga för att förebygga brott eller hot mot ordningen och säkerheten vid evenemanget. Detta informationsutbyte bedöms kunna regleras i förordning. Skyldigheten att praktiskt bistå en annan medlemsstat för att förebygga brott eller förhindra ordningsstörningar vid evenemang med gränsöverskridande verkningar, katastrofer och allvarliga olyckor föreslås också genomföras i förordning.

Eftersom den information som utbyts ska kunna förses med villkor för användningen föreslås en ny bestämmelse som ger svenska myndigheter möjlighet att ställa villkor när uppgifter eller bevismaterial överlämnas till en utländsk myndighet eller mellanfolklig organisation inom ramen för internationellt polissamarbete. Motsvarande gäller redan för en utländsk myndighet eller mellanfolklig organisation i förhållande till svenska myndigheter.

Främst mot bakgrund av att Norge och Island har begärt att få delta i samarbetet enligt Prümrådsbeslutet och att förhandlingar om associeringsavtal pågår, har lagförslagen utformats generellt, dvs. bestämmelserna ska kunna tillämpas i förhållande till en annan stat oavsett om staten är medlem i Europeiska unionen eller inte.

Allt informationsutbyte enligt rådsbeslutet ska gå genom ett nationellt kontaktställe. Rikspolisstyrelsen föreslås bli svenskt kontaktställe.

Informationsutbytet ska övervakas av nationella tillsynsmyndigheter. Det föreslås att Datainspektionen utses till tillsynsmyndighet enligt rådsbeslutet.

2 Författningsförslag

2.1 Förslag till lag om ändring i polisdatalagen (1998:622)

Härigenom föreskrivs

dels att 1, 3, 22–27 a och 29 §§ polisdatalagen (1998:622) ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 27 b och 31 a §§, av följande lydelse,

dels att två nya rubriker ska införas närmast före 27 b och 31 a §§ av följande lydelse,

dels att punkten 2 i ikraftträdande- och övergångsbestämmelserna till polisdatalagen ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

1 §[1]

Denna lag gäller utöver personuppgiftslagen (1998:204) vid behandling av personuppgifter i polisens verksamhet och i polisverksamhet vid Ekobrottsmyndigheten för att

1. förebygga brott och andra störningar av den allmänna ordningen och säkerheten,

2. övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när sådana har inträffat eller

[1] Senaste lydelse 2006:446.

3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

Lagen gäller också behandling av sådana uppgifter som avses i 25 och 26 §§.

Lagen gäller inte för behandling av personuppgifter som företas med stöd av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem eller lagen (2006:444) om passagerarregister.

I lagen (2000:343) om internationellt polisiärt samarbete och föreskrifter som har meddelats med stöd av den lagen finns särskilda bestämmelser om behandling av personuppgifter med stöd av Europeiska rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet som gäller utöver denna lag.

3 §

I denna lag avses med

underrättelseverksamhet: polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap. rättegångsbalken,

kriminalunderrättelseverksamhet: annan underrättelseverksamhet än den som bedrivs av Säkerhetspolisen,

allvarlig brottslig verksamhet: verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver,

särskild undersökning: en undersökning i kriminalunderrättelseverksamhet som innebär insamling, bearbetning och analys av

uppgifter i syfte att ge underlag för beslut om förundersökning eller om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott,

DNA-analys: varje förfarande som kan användas för analys av deoxyribonukleinsyra.	*DNA-analys*: varje förfarande som kan användas för analys av deoxyribonukleinsyra *i humant material*,
	DNA-profil: resultatet av en DNA-analys som presenteras i form av siffror eller bokstäver.

De begrepp som i övrigt används i denna lag har samma betydelse som i personuppgiftslagen (1998:204).

22 §[2]

Uppgifter om resultat av DNA-analyser får behandlas endast för att underlätta identifiering av personer i samband med utredning av brott. Rikspolisstyrelsen får föra register (*DNA-register*, *utredningsregister* och *spårregister*) i enlighet med 23–27 §§ över de uppgifter som behandlas.	*DNA-profiler* får behandlas endast för att underlätta identifiering av personer i samband med utredning av brott. Rikspolisstyrelsen får föra register (*DNA-registret*, *utredningsregistret* och *spårregistret*) i enlighet med 23–27 §§ över de uppgifter som behandlas.
Sådana uppgifter som avses i första stycket får även behandlas i förundersökningar och särskilda undersökningar.	*DNA-profiler* får även behandlas i förundersökningar och särskilda undersökningar. *Detsamma gäller om behandlingen är nödvändig för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.*

[2] Senaste lydelse 2005:877.

23 §[3]

Ett DNA-register får innehålla *uppgifter om resultatet av* DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som

1. genom lagakraftvunnen dom har dömts till annan påföljd än böter, eller

2. har godkänt ett strafföreläggande som avser villkorlig dom.

DNA-registret får innehålla *DNA-profiler från* DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som

1. genom lagakraftvunnen dom har dömts till annan påföljd än böter, eller

2. har godkänt ett strafföreläggande som avser villkorlig dom.

24 §

Registreringen av *ett analysresultat skall begränsas till uppgifter som ger* information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får inte registreras.

Utöver vad som sägs i första stycket får DNA-registret endast innehålla *upplysningar som visar* i vilket ärende *analysen har gjorts* och vem *analysen* avser.

Registreringen av *en DNA-profil får endast ge* information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får inte registreras.

Utöver *DNA-profiler* får DNA-registret endast innehålla *uppgifter om* i vilket ärende *DNA-profilen har tagits fram* och vem *profilen* avser.

[3] Senaste lydelse 2005:877.

24 a §[4]

Ett utredningsregister får innehålla *uppgifter om resultatet av* DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för ett brott på vilket fängelse kan följa.	*Utredningsregistret* får innehålla *DNA-profiler från* DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för ett brott på vilket fängelse kan följa.
Vad som anges i 24 § gäller också vid registrering i utredningsregistret.	

25 §

Ett spårregister får innehålla *uppgifter om DNA-analyser* som har *gjorts* under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver *uppgifter om analysresultat* får *ett spårregister* endast innehålla *upplysningar som visar* i vilket ärende *analysen* har gjorts.	*Spårregistret* får innehålla *DNA-profiler* som har *analyserats* under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver *DNA-profiler* får *spårregistret* endast innehålla *uppgifter om i* vilket ärende *DNA-analysen* har gjorts.

26 §[5]

Uppgifter i spårregister får endast jämföras med *analysresultat*	*DNA-profiler i spårregistret* får endast jämföras med *DNA-profiler*
1. som inte kan hänföras till en identifierbar person,	1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller	2. som finns i DNA-registret, eller

[4] Senaste lydelse 2005:877.
[5] Senaste lydelse 2005:877.

3. som kan hänföras till en person som är skäligen misstänkt för brott.	3. som kan hänföras till en person som är skäligen misstänkt för brott.
	DNA-profiler i spårregistret får också jämföras om det är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.
27 §[6]	
Uppgifter i DNA-registret *skall* gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.	Uppgifter i DNA-registret *ska* gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.
Uppgifter i utredningsregistret *skall* gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade godkänt ett strafföreläggande som avser enbart böter.	Uppgifter i utredningsregistret *ska* gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade godkänt ett strafföreläggande som avser enbart böter.
Uppgifter i *spårregister skall* gallras senast trettio år efter registreringen.	Uppgifter i *spårregistret ska* gallras senast trettio år efter registreringen.

[6] Senaste lydelse 2005:877.

27 a §[7]

Ett prov för DNA-analys som har tagits med stöd av bestämmelserna i 28 kap. 12–12 b §§ rättegångsbalken *skall* förstöras senast sex månader efter det att provet togs.

Om uppgifterna i utredningsregistret *skall* gallras vid en tidigare tidpunkt *enligt 27 §*, *skall* även det prov som avser den registrerade förstöras senast vid samma tidpunkt.

Om *provet* har tagits från någon som inte är skäligen misstänkt för brott, *skall* provet förstöras *så snart målet eller ärendet slutligt har avgjorts*.

Ett prov för DNA-analys som har tagits med stöd av bestämmelserna i 28 kap. 12–12 b §§ rättegångsbalken *ska* förstöras senast sex månader efter det att provet togs, *om inte annat sägs i andra–fjärde stycket*.

I de fall uppgifterna i utredningsregistret *om en registrerad person enligt 27 § ska* gallras vid en tidigare tidpunkt *än som anges i första stycket*, *ska* även prov *från denne* förstöras senast vid samma tidpunkt.

Om *prov* har tagits från någon som inte är skäligen misstänkt för brott, *och målet eller ärendet avgörs slutligt vid en tidigare tidpunkt än som sägs i första stycket, ska även* provet förstöras *senast vid den tidigare tidpunkten.*

Prov som tagits på begäran av en annan stat ska förstöras senast två månader efter det att provet togs.

[7] Senaste lydelse 2005:877.

Direktåtkomst

27 b §

I lagen (2000:343) om internationellt polisiärt samarbete finns bestämmelser om direktåtkomst till uppgifter i DNA-registret, utredningsregistret och spårregistret vid samarbete med stöd av Europeiska rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet.

29 §

För att underlätta identifiering av personer i samband med brott får Rikspolisstyrelsen behandla uppgifter i fingeravtrycks- och signalementsregister. Ett sådant register får användas för identifiering av okända personer även i andra fall.

Sådana uppgifter som avses i första stycket får även behandlas i förundersökningar och särskilda undersökningar.

Uppgifter i fingeravtrycksregister får också behandlas om detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Direktåtkomst

31 a §

I lagen (2000:343) om internationellt polisiärt samarbete finns bestämmelser om direktåtkomst till uppgifter i fingeravtrycksregister vid samarbete med stöd av Europeiska rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet.

2.[8] För de personregister som den 24 oktober 1998 förs med Datainspektionens tillstånd gäller bestämmelserna i datalagen (1973:289) till och med den 31 december 2009.

2. För de personregister som den 24 oktober 1998 förs med Datainspektionens tillstånd gäller bestämmelserna i datalagen (1973:289) till och med den 31 december 2009. *För fingeravtrycksregister ska dock 29–31 §§ gälla från ikraftträdandet.*

Denna lag träder i kraft den …

[8] Senaste lydelse 2008:880.

2.2 Förslag till lag om ändring i lagen (2000:343) om internationellt polisiärt samarbete

Härigenom föreskrivs

dels att 2, 3 och 11–13 §§ lagen (2000:343) om internationellt polisiärt samarbete ska ha följande lydelse,

dels att rubriken före 11 § ska ha följande lydelse,

dels att det i lagen ska införas sex nya paragrafer, 3 a och 16–20 §§ av följande lydelse,

dels att det ska införas nya rubriker före 16, 18 och 20 §§ med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 §
I denna lag avses med	
– *utländska tjänstemän:* utländska polismän och andra utländska tjänstemän som har anmälts vara behöriga att utföra sådant gränsöverskridande arbete som avses i artikel 40 och 41 i konventionen om tillämpning av Schengenavtalet av den 14 juni 1985 (Schengenkonventionen),	
– *förföljande tjänstemän:* utländska tjänstemän som förföljer en person på svenskt territorium enligt denna lag,	
– *svenska tjänstemän:* svenska polismän, tulltjänstemän eller kustbevakningstjänstemän när de enligt lag eller annan författning har polisiära befogenheter,	
– *Öresundsförbindelsen:* den fasta förbindelsen över Öresund som den definieras i artikel 2 i avtalet av den 6 oktober 1999 mellan Konungariket Sveriges regering och Konungariket Danmarks regering om polisiärt samarbete i Öresundsregionen,	
	– *Prümrådsbeslutet: Europeiska rådets beslut 2008/615/RIF av den 23 juni 2008 om ett för-*

djupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet,

– kontaktställe: sådan nationell kontaktpunkt som anmälts som behörig för förmedling av uppgifter enligt artikel 6, 11 och 12 i Prümrådsbeslutet,

– referensuppgifter: sådana registeruppgifter som inte röjer identiteten på den person som uppgifterna avser.

3 §

Har en svensk myndighet fått upplysningar eller bevismaterial från *en annan stat* för att användas i underrättelseverksamhet om brott eller vid utredning av brott och gäller på grund av en överenskommelse med den *andra staten* villkor som begränsar möjligheten att utnyttja materialet, *skall* svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning.

Har en svensk myndighet fått upplysningar eller bevismaterial från, *eller har detta gjorts tillgängligt av,*

1. en annan stat, eller

2. en mellanfolklig organisation

för att användas i underrättelseverksamhet om brott, vid utredning av brott, eller för att upprätthålla allmän ordning och säkerhet, och gäller på grund av en överenskommelse med den som tillhandahållit materialet villkor som begränsar möjligheten att utnyttja detta, ska svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning.

Bestämmelserna i första stycket gäller också i fråga om överenskommelser med mellanfolkliga organisationer.

3 a §

Upplysningar eller bevismaterial som en svensk brottsbekämpande myndighet lämnar till, eller gör tillgängligt för,

1. en annan stat, eller

2. en mellanfolklig organisation

får i enskilda fall förenas med villkor som begränsar möjligheten att utnyttja materialet, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige.

Gemensamma bestämmelser

Gemensamma bestämmelser *för samarbete enligt Schengenkonventionen och inom Öresundsregionen*

11 §

Utländska tjänstemän *skall*, när de utövar befogenheter enligt *denna lag*, följa svensk lag och annan författning samt instruktioner som meddelas av behöriga svenska polismyndigheter. Under gränsöverskri-

Utländska tjänstemän *ska*, när de utövar befogenheter enligt *4–9 §§*, följa svensk lag och annan författning samt instruktioner som meddelas av behöriga svenska polismyndigheter. Under gränsöverskri-

dande förföljande eller övervakning får de inte beträda bostäder eller andra platser som inte är öppna för allmänheten. Tjänstevapen får bara användas i nödvärnssituationer. Utländska tjänstemän *skall* alltid kunna styrka sin behörighet och identitet.	dande förföljande eller övervakning får de inte beträda bostäder eller andra platser som inte är öppna för allmänheten. Tjänstevapen får bara användas i nödvärnssituationer. Utländska tjänstemän *ska* alltid kunna styrka sin behörighet och identitet.

Att undantag kan göras från vapenlagens (1996:67) bestämmelser, i fråga om rätt för företrädare för främmande stats myndighet att medföra skjutvapen och ammunition vid tillfällig tjänstgöring i Sverige, följer av 11 kap. 1 § f sagda lag.

12 §

Utländska tjänstemän som utövar myndighet enligt *denna lag* i Sverige *skall* vara skyddade enligt 17 kap. 1, 2 och 4 §§ brottsbalken på motsvarande sätt som om det varit fråga om svensk myndighetsutövning.	Utländska tjänstemän som utövar myndighet enligt *4–9 §§* i Sverige *ska* vara skyddade enligt 17 kap. 1, 2 och 4 §§ brottsbalken på motsvarande sätt som om det varit fråga om svensk myndighetsutövning.
Utländska tjänstemän som utövar myndighet enligt *denna lag* i Sverige *skall* vara ansvariga för tjänstefel enligt 20 kap. 1 § brottsbalken på motsvarande sätt som om det varit fråga om svensk myndighetsutövning.	Utländska tjänstemän som utövar myndighet enligt *4–9 §§* i Sverige *ska* vara ansvariga för tjänstefel enligt 20 kap. 1 § brottsbalken på motsvarande sätt som om det varit fråga om svensk myndighetsutövning.

13 §

Om utländska tjänstemän utför uppgifter enligt *denna lag* i Sverige, *skall* svenska staten i stället för den utländska myndigheten eller tjänstemannen	Om utländska tjänstemän utför uppgifter enligt *4–9 §§* i Sverige, *ska* svenska staten i stället för den utländska myndigheten eller tjänstemannen

ersätta skada som uppkommer i samband med förföljandet, övervakningen eller ingripandet i övrigt och för vilken den utländska myndigheten eller tjänstemannen skulle ha varit skadeståndsskyldig om svensk lag varit tillämplig på dem. Svenska staten *skall* dock inte ersätta skada som uppkommer hos den utländska myndigheten eller tjänstemannen.

ersätta skada som uppkommer i samband med förföljandet, övervakningen eller ingripandet i övrigt och för vilken den utländska myndigheten eller tjänstemannen skulle ha varit skadeståndsskyldig om svensk lag varit tillämplig på dem. Svenska staten *ska* dock inte ersätta skada som uppkommer hos den utländska myndigheten eller tjänstemannen.

Samarbete med stöd av Prümrådsbeslutet

Utbyte av DNA-profiler

16 §

Vid samarbete med stöd av Prümrådsbeslutet får ett kontaktställe i en annan stat medges direktåtkomst till referensuppgifter i DNA-registret, spårregistret och utredningsregistret.

Ett sådant kontaktställe får i samband med brottsutredning i ett enskilt fall behandla referensuppgifter om DNA-profiler i dessa register. Efter överenskommelse mellan Sverige och en annan stat får kontaktstället i en annan stat även göra automatisk jämförelse mellan egna oidentifierade DNA-profiler och referensuppgifter avseende DNA-

profiler i svenska DNA-register.

Rikspolisstyrelsen får ingå en sådan överenskommelse som anges i andra stycket.

17 §

Vid förundersökning eller annan utredning enligt bestämmelserna om förundersökning i brottmål får det svenska kontaktstället i ett enskilt fall, för de ändamål och med de begränsningar som anges i 22–26 §§ polisdatalagen (1998:622), behandla uppgifter i en annan stats DNA-register. Behandling får endast ske i den utsträckning den andra staten tillåter det.

Efter överenskommelse med en annan stat får det svenska kontaktstället göra en automatisk jämförelse mellan DNA-profiler i spårregistret och referensuppgifter avseende DNA-profiler i den andra statens DNA-register.

Rikspolisstyrelsen får ingå en sådan överenskommelse som anges i andra stycket.

Utbyte av fingeravtryck

18 §

Vid samarbetet med stöd av Prümrådsbeslutet får ett kontaktställe i en annan stat medges direktåtkomst till referensuppgifter i svenska fingeravtrycksregister. Kontaktstället får i ett enskilt fall behandla referensuppgifter för att förebygga och utreda brott.

19 §

För att förebygga eller utreda brott får, för de ändamål och med de begränsningar som anges i 29–31 §§ polisdatalagen (1998:622), det svenska kontaktstället behandla uppgifter i en annan stats fingeravtrycksregister, i den utsträckning den andra staten tillåter det.

Övriga bestämmelser

20 §

Närmare bestämmelser om förfarandet vid samarbete med stöd av Prümrådsbeslutet finns i förordning.

Denna lag träder i kraft den …

2.3 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs att det i lagen (2000:562) om internationell rättslig hjälp i brottmål

dels ska införas två nya paragrafer, 4 kap. 24 a och b §§, med följande lydelse,

dels ska införas nya rubriker omedelbart före 4 kap. 24 a och 24 b §§ med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	Framtagande av DNA-profil
	24 a §
	Pågår en brottsutredning eller något annat straffrättsligt förfarande i en annan stat mot en person som vistas i Sverige, ska, på begäran av den andra staten, rättslig hjälp ges med tagande av DNA-prov och analys av provet, om
	1. DNA-profil på personen saknas,
	2. den ansökande staten anger för vilket ändamål DNA-profilen behövs, och
	3. det av ansökan framgår att det hade funnits förutsättningar för att vidta sådan åtgärd om

personen hade vistats i den ansökande staten.

DNA-profilen översänds i form av siffror eller bokstäver.

Begäran om DNA-profil

24 b §

Under en förundersökning eller annan utredning enligt bestämmelserna om förundersökning i brottmål, som rör en person som vistas i en annan stat, får rättslig hjälp begäras med tagande av DNA-prov från denne och med analys av provet. En sådan ansökan ska innehålla uppgifter om

1. att DNA-profil för personen saknas,

2. det ändamål för vilket DNA-profilen behövs, och

3. huruvida det funnits förutsättningar för att vidta en sådan åtgärd om personen hade vistats i Sverige.

Denna lag träder i kraft den …

2.4 Förslag till lag om ändring i lagen (2001:558) om vägtrafikregister

Härigenom föreskrivs att 2, 5 och 8 §§ lagen (2001:558) om vägtrafikregister ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §	
I personuppgiftslagen (1998:204) finns bestämmelser som tillämpas på personuppgifter i vägtrafikregistret i den mån det inte finns några avvikande bestämmelser i denna lag eller i *en* förordning *som har beslutats med stöd av den.*	I personuppgiftslagen (1998:204) finns bestämmelser som tillämpas på personuppgifter i vägtrafikregistret i den mån det inte finns några avvikande bestämmelser i denna lag eller i förordning.

Med personuppgifter avses i denna lag detsamma som i personuppgiftslagen.

5 §[1]	
I fråga om personuppgifter *skall* vägtrafikregistret ha till ändamål att tillhandahålla uppgifter för	I fråga om personuppgifter *ska* vägtrafikregistret ha till ändamål att tillhandahålla uppgifter för

1. verksamhet, för vilken staten eller en kommun ansvarar enligt lag eller annan författning, i fråga om

a) fordonsägare,

b) den som ansöker om, har eller har haft behörighet att framföra fordon eller luftfartyg enligt körkortslagen (1998:488), yrkestrafiklagen (1998:490), luftfartslagen (1957:297) eller nå-

[1] Senaste lydelse 2007:1159.

gon annan författning eller den som har rätt att utöva viss tjänst enligt luftfartslagen,

c) annan person om det behövs för att underlätta handläggningen av ett körkorts- eller yrkestrafikärende,

d) den som ansöker om, har eller har haft tillstånd att bedriva yrkesmässig trafik enligt yrkestrafiklagen eller någon annan författning eller biluthyrning enligt lagen (1998:492) om biluthyrning,

e) den som ansöker om, har eller har haft färdskrivarkort som avses i rådets förordning (EEG) nr 3821/85 av den 20 december 1985 om färdskrivare vid vägtransporter, eller

f) den som har eller har haft yrkeskompetens att utföra transporter enligt lagen (2007:1157) om yrkesförarkompetens eller genomgår utbildning för att få sådan kompetens,

2. försäkringsgivning eller annan allmän eller enskild verksamhet där uppgifter om personer under 1 a), b) och d) utgör underlag för prövningar eller beslut,

3. information om fordonsägare för trafiksäkerhets- eller miljöändamål och för att i den allmänna omsättningen av fordon förebygga brott samt information om den som har behörighet att framföra fordon för att utreda trafikbrott i samband med automatisk trafiksäkerhetskontroll,

4. aktualisering, komplettering eller kontroll av information om fordonsägare som finns i kund- eller medlemsregister eller liknande register,

5. uttag av urval för direkt marknadsföring av information om fordonsägare, dock med den begränsning som följer av 11 § personuppgiftslagen (1998:204), samt

6. en utländsk myndighets inhämtande, i enlighet med en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt, av uppgifter om fordon och fordons ägare eller innehavare, i syfte att användas i myndighetens verk-

	samhet för att förebygga brott, utreda brott eller upprätthålla allmän säkerhet.
8 §	
Direktåtkomst till personuppgifter får medges endast för sådana ändamål som anges i 5 § 1–3 i enlighet med föreskrifter meddelade av regeringen.	Direktåtkomst till personuppgifter får medges endast för sådana ändamål som anges i 5 § 1–3 *och 6* i enlighet med föreskrifter meddelade av regeringen.

Denna lag träder i kraft den …

2.5 Förslag till förordning om ändring i förordningen (2000:388) om internationellt polisiärt samarbete

Härigenom föreskrivs att det i förordningen (2000:388) om internationellt polisiärt samarbete

dels ska införas 19 nya paragrafer, 3–21 §§, med följande lydelse,

dels ska införas nya rubriker omedelbart före 3, 4, 5, 7, 8, 9, 10, 14, 16, 19 och 20 §§, med följande lydelser.

Nuvarande lydelse	*Föreslagen lydelse*
	Samarbete enligt Prümrådsbeslutet
	Nationellt kontaktställe
	3 §
	Rikspolisstyrelsen ska vara kontaktställe enligt Prümrådsbeslutet för förmedling av uppgifter ur DNA-register, fingeravtrycksregister och vägtrafikregistret samt av framtagna DNA-profiler.
	Automatiskt meddelande
	4 §
	Vid behandling av uppgifter enligt 16 § andra stycket och 18 § lagen (2000:343) om in-

ternationellt polisiärt samarbete, ska ett automatiskt meddelande genereras om huruvida den sökta DNA-profilen eller det sökta fingeravtrycket förekommer i registret eller inte.

Förekommer DNA-profilen eller fingeravtrycket ska kontaktstället i den andra staten automatiskt få del av referensuppgifter i form av den ickekodifierade delen av DNA-profilen respektive fingeravtrycksuppgiften och en sifferbeteckning.

Informationsutbyte vid större evenemang med gränsöverskridande verkningar

5 §

Vid större nationella eller utländska evenemang med gränsöverskridande verkningar ska det svenska kontaktstället på begäran av en annan stat, eller på eget initiativ, i brottsförebyggande eller ordningshållande syfte översända

1. personuppgifter gällande personer som det finns skäl att anta kan komma att begå brott vid evenemanget, eller som kan utgöra hot mot den allmänna ordningen och säkerheten vid

detta, eller

2. andra uppgifter som bedöms vara nödvändiga för att förebygga brott eller hot mot den allmänna ordningen och säkerheten vid evenemanget.

Första stycket gäller dock inte om uppgifterna enligt lag eller annan författning inte får lämnas ut.

6 §

Om en svensk myndighet i samband med större evenemang med gränsöverskridande verkningar från en annan stat mottar personuppgifter avseende personer som det finns skäl att anta kan komma att begå brott vid evenemanget, eller som kan utgöra hot mot den allmänna ordningen och säkerheten vid detta, får uppgifterna bevaras endast så länge de behövs för att uppnå det syfte för vilket de mottogs eller när detta syfte inte längre kan uppnås. Uppgifterna ska därefter utplånas. De får längst bevaras ett år efter översändandet.

Bistånd vid större evenemang, katastrofer och allvarliga olyckor

7 §

I syfte att förhindra brott eller upprätthålla allmän ordning och säkerhet vid större evenemang och liknande viktiga händelser, katastrofer och allvarliga olyckor som har gränsöverskridande verkningar, ska det svenska kontaktstället så tidigt som möjligt underrätta en annan stat om situationen och förmedla väsentlig information om denna.

Berörd polismyndighet ska omedelbart underrätta Rikspolisstyrelsen om situationer med gränsöverskridande verkningar. Styrelsen ska samordna nödvändiga polisiära åtgärder.

Rikspolisstyrelsen får i sådana situationer som anges i andra stycket, på begäran av den stat på vars territorium situationen uppstått, besluta om att polisväsendet ska tillhandahålla den andra staten tjänstemän, specialister och rådgivare samt nödvändig utrustning.

Allmänna bestämmelser om utplåning

8 §

Personuppgifter som med stöd av Prümrådsbeslutet har översänts från, eller gjorts tillgängliga av, en annan stat ska utplånas om uppgifterna

1. är felaktiga,

2. inte borde ha översänts,

3. har översänts och mottagits korrekt, men inte längre är nödvändiga för det ändamål för vilket de översändes, eller

4. har överskridit den längsta lagringstid som en utländsk myndighet i samband med översändandet har angett vara tillåten enligt den statens lagstiftning.

Spärrning och märkning

9 §

I stället för att utplåna uppgifter enligt 8 § 2–4 ska uppgifterna förses med information om att de är spärrade, om utplåning skulle innebära skada för den person som uppgifterna rör. Sådana uppgifter får endast behandlas för samma syfte som förhindrade utplåning.

Personuppgifter ska märkas

på begäran av den person som uppgifterna rör, om han eller hon bestrider att personuppgifterna är korrekta och uppgifternas korrekthet inte kan fastställas.

Registreringsskyldighet

10 §

Personuppgifter som översänds eller mottas med stöd av Prümrådsbeslutet ska registreras enligt 11 och 12 §§.

11 §

Vid varje översändande eller mottagande på annat sätt än genom direktåtkomst av sådana uppgifter som avses i 10 §, ska kontaktstället och det organ som administrerar databasen registrera

1. skälet till översändandet,

2. vilka uppgifter som har översänts eller mottagits,

3. datum för översändandet,

4. namn eller beteckning på det sökande organet, och

5. vem som administrerar databasen.

12 §

Vid varje översändande eller mottagande genom direktåtkomst av sådana uppgifter som

avses i 10 § ska kontaktstället och det organ som administrerar databasen registrera

1. om sökningen har lett till överensstämmelse med uppgift i registret eller inte,

2. vilka uppgifter som har översänts,

3. datum och exakt tidpunkt för översändandet,

4. namn eller beteckning på det sökande organet, och

5. vem som administrerar databasen.

Vid en sökning i ett register som förs av en annan stat ska kontaktstället registrera syftet med sökningen och vilken tjänsteman som beslutat om denna.

13 §

Uppgifter som har registrerats enligt 11 eller 12 § ska gallras senast två år efter registreringen.

Underrättelse- och informationsskyldighet

14 §

Har det visat sig att uppgifter som med stöd av Prümrådsbeslutet har översänts från Sverige till en annan stat är felaktiga, eller att de inte borde ha över-

sänts, ska det svenska kontaktstället underrätta mottagaren av uppgifterna.

En myndighet, som finner att sådana uppgifter som sägs i första stycket är felaktiga eller inte borde ha översänts, ska underrätta kontaktstället om detta.

15 §

På begäran av kontaktstället i en stat som översänt uppgifter, ska det svenska kontaktstället informera om behandlingen av mottagna uppgifter och de resultat som har erhållits.

På begäran av en berörd stats dataskyddsmyndighet ska det svenska kontaktstället, utan dröjsmål och senast inom fyra veckor, översända de uppgifter som registrerats enligt 11 och 12 §§.

Tillsynsmyndighetens uppgifter

16 §

Datainspektionen är tillsynsmyndighet.

Datainspektionen ska

1. utföra kontroller av behandling med stöd av Prümrådsbeslutet, på eget initiativ eller efter anmodan av en dataskyddsmyndighet i en annan stat,

2. förvara resultaten av sådana kontroller i arton månader för att därefter omedelbart utplåna dessa, och

3. på begäran, utan dröjsmål och senast inom fyra veckor, översända uppgifter om resultaten av kontrollerna till en dataskyddsmyndighet i berörd stat.

17 §

Om en personuppgift har försetts med märkning enligt 9 § andra stycket och dess korrekthet har kunnat fastställas, får Datainspektionen, på begäran av den som uppgiften rör eller den myndighet som bevarar uppgiften, besluta att märkningen ska avlägsnas.

18 §

Datainspektionen får av en myndighet i en annan stat, som med stöd av Prümrådsbeslutet har behandlat personuppgifter som härrör från Sverige, begära de uppgifter om behandlingen som ska registreras.

Datainspektionen får anmoda en dataskyddsmyndighet i en annan stat att genomföra nödvändiga inspektioner för kontroll av behandlingen av personuppgifter som härrör från Sverige och som sker med stöd av Prümrådsbeslutet.

Överklagande

19 §

Beslut enligt 17 § får överklagas hos allmän förvaltningsdomstol enligt 22 a § förvaltningslagen (1986:223).

Övriga bestämmelser

20 §

Rikspolisstyrelsen ska i särskilda beslut ange vilka tjänstemän som får genomföra sökningar som anges i 17 § första och andra stycket och 19 § lagen (2000:343) om internationellt polisiärt samarbete.

På begäran av en svensk tillsynsmyndighet eller en dataskyddsmyndighet i en annan stat ska kontaktstället lämna uppgift om vilka tjänstemän som är behöriga.

21 §

Rikspolisstyrelsen får meddela de ytterligare föreskrifter som behövs för verkställighet av 16–19 §§ lagen (2000:343) om internationellt polisiärt samarbete samt 5, 7, 11–15 och 20 §§ denna förordning.

Denna förordning träder i kraft den…

3 Innehållet i rådsbeslutet

3.1 Allmän bakgrund

Det s.k. Prümfördraget ingicks i maj 2005 mellan Beneluxländerna, Tyskland, Spanien, Frankrike och Österrike för att utveckla informationsutbytet mellan vissa stater, framför allt vad gäller DNA-, fingeravtrycks- och fordonsuppgifter. Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet[1] (det s.k. Prümrådsbeslutet) bygger vidare på merparten av Prümfördragets bestämmelser, men nu som ett instrument för Europeiska unionen.

I maj 2008 godkände riksdagen utkastet till Prümrådsbeslut.[2] Prümrådsbeslutet antogs av rådet den 23 juni 2008. Samma dag antogs även rådets beslut 2008/616/RIF av den 23 juni 2008 om genomförande av beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet[3] (i fortsättningen kallat genomförandebeslutet).

Prümrådsbeslutet syftar till att fördjupa det gränsöverskridande samarbetet mellan myndigheter inom Europeiska unionen som ansvarar för att förebygga och utreda brott. Det brottsbekämpande och brottsförebyggande arbetet ska bl.a. underlättas genom ett utvecklat informationsutbyte och tillgång till sådana uppgifter i andra medlemsstaters DNA-, fingeravtrycks- och

[1] EUT 6.8.2008, L 210 s. 1.
[2] Prop. 2007/08:83, bet. 2007/08:JuU20, rskr. 2007/08:197.
[3] EUT 6.8.2008, L 210 s. 12.

fordonsregister som inte röjer någons identitet. Rådsbeslutet reglerar också utbyte av information vid större evenemang med gränsöverskridande verkningar och uppgiftsutbyte för att bekämpa terrorism. Även möjligheten att genom gemensamma insatser fördjupa polissamarbetet samt medlemsstaternas skyldighet att bistå varandra praktiskt vid större evenemang, katastrofer och allvarliga olyckor behandlas i rådsbeslutet.

3.2 Rådsbeslutets uppbyggnad

Rådsbeslutet är indelat i sju kapitel och omfattar 37 artiklar.

I preambeln framhålls att beslutet syftar till att införliva innebörden av bestämmelserna i Prümfördraget med Europeiska unionens lagstiftning. Vidare hänvisas till bl.a. Haagprogrammet (se avsnitt 4.1) och rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (det s.k. svenska initiativet, se avsnitt 4.2.4).

Preambeln betonar bl.a. att rådsbeslutet bygger på att man inrättar nätverk mellan medlemsstaternas egna databaser och utgår från ett system med ”träff, icke träff” (”hit, no-hit”). Systemet innebär att endast icke identitetsanknutna (”anonyma”) fingeravtrycksuppgifter och DNA-profiler jämförs. Frågan om utbyte av ytterligare personuppgifter efter en träff regleras nationellt. På detta sätt, och med utgångspunkten att översändande av personuppgifter till en annan medlemsstat förutsätter att dataskyddet i den mottagande medlemsstaten är tillfredsställande, ska skyddet av personuppgifter garanteras (skäl 10 och 18).

I rådsbeslutets *kapitel 1* behandlas dess syfte och tillämpningsområde. I *kapitel 2* finns bestämmelser om elektronisk tillgång till uppgifter om DNA-analyser, fingeravtrycksuppgifter och fordonsuppgifter. *Kapitel 3* reglerar informationsutbyte i samband med större evenemang och *kapitel 4* informationsutbyte för att förebygga terroristbrott. *Kapitel 5* reglerar andra for-

mer av samarbete, bl.a. gemensamma polisiära insatser. *Kapitel 6* behandlar dataskyddet för uppgifter som översänds eller har översänts. I *kapitel 7* finns genomförande- och slutbestämmelser.

Med stöd av artikel 33 i rådsbeslutet har rådet, som nyss nämnts, meddelat bestämmelser för det administrativa och tekniska genomförandet. Genomförandebeslutet reglerar framför allt det automatiska utbytet av uppgifter i DNA-, fingeravtrycks- och fordonsregister. I en bilaga till genomförandebeslutet finns detaljbestämmelser av teknisk karaktär.

I det följande redovisas i första hand innehållet i rådsbeslutet. Avgränsningen av uppdraget (se *bilaga 1*) medför att rådsbeslutets fakultativa bestämmelser om gemensamma insatser kommer att utredas i särskild ordning (främst artiklarna 17 och 19 och delar av artikel 21). Genomgången i detta avsnitt omfattar trots detta hela rådsbeslutet. Även genomförandebeslutet behandlas i vissa delar.

3.3 Syfte och tillämpningsområde

Artikel 1 lägger fast rådsbeslutets syfte och tillämpningsområde. Genom rådsbeslutet har medlemsstaterna för avsikt att fördjupa det gränsöverskridande samarbete som omfattas av avdelning VI i fördraget om Europeiska unionen (bestämmelser om polissamarbete och straffrättsligt samarbete), särskilt i fråga om utbyte av information mellan myndigheter som är ansvariga för att förebygga och utreda brott.

3.4 Åtkomst on-line och begäran om uppföljning

Artiklarna 2–7 reglerar i huvudsak nationella register för DNA-analyser och utbyte av uppgifter ur sådana register.

3.4.1 DNA-profiler

Nationella DNA-register

I varje medlemsstat ska det finnas nationella register med DNA-analyser för brottsutredningar (artikel 2.1). Den behandling som krävs enligt rådsbeslutet ska utföras enligt bestämmelserna i beslutet och i överensstämmelse med nationell rätt.

Medlemsstaterna ska bereda varandra tillgång till referensuppgifter i sina DNA-register (artikel 2.2). Det ska inte vara möjligt att omedelbart kunna identifiera vilken person referensuppgifterna hänför sig till. Referensuppgifterna får därför enbart innehålla DNA-profiler från den icke-kodifierade delen av DNA:t och en sifferbeteckning. Referensuppgifter som inte kan kopplas till en viss person (oidentifierade DNA-profiler) ska kunna identifieras som sådana.

De sifferbeteckningar som avses ska enligt genomförandebeslutet bestå av en kombination av dels en kod som gör det möjligt för medlemsstaterna att, om en överensstämmelse konstaterats, hämta personuppgifter och ytterligare information från sina databaser för eventuell vidarebefordran till en, flera eller samtliga medlemsstater, dels en kod för att ange DNA-profilens nationella ursprung, dels en kod för att ange typen av DNA-profil (artikel 6 genomförandebeslutet).

Medlemsstaterna ska underrätta rådets generalsekretariat om vilka nationella register över DNA-analyser som omfattas av artiklarna 2–6 (artikel 2.3).

Automatisk sökning

En automatisk sökning innebär att medlemsstaterna ska ge varandra tillträde till DNA-profiler med tillhörande sifferuppgift i DNA-register (artikel 3.1). Den utländska myndigheten ska ges direktåtkomst till en annan medlemsstats databas och en förfrågan ska besvaras automatiskt (se vidare definitionen i artikel 24).

Sökningar får dock endast göras i samband med brottsutredningar, i enskilda fall och enligt lagstiftningen i den medlemsstat som genomför sökningen. Utbytet ska ske genom särskilt utsedda nationella kontaktställen.

Den myndighet som har gjort sökningen ska automatiskt underrättas om en träff, och i så fall få referensuppgifter, eller i stället få besked om att ingen träff uppkommit (artikel 3.2). Detta s.k. ”träff, ingen träff-system” eller ”hit, no hit-system” utvecklas närmare i artiklarna 9 och 10 i genomförandebeslutet.

I artikel 8 i genomförandebeslutet preciseras vilken information en begäran om automatisk sökning enligt artikel 3 och ett svar ska innehålla.

Automatisk jämförelse

För att det ska vara möjligt att jämföra ett lands samtliga oidentifierade DNA-profiler (s.k. öppna spår) med referensuppgifterna i ett annat lands DNA-register får också automatiska jämförelser göras (artikel 4). Till skillnad från en automatisk sökning (artikel 3) sker jämförelsen inte i enskilda fall. Jämförelsen förutsätter att en överenskommelse först har träffats mellan berörda stater samt att sökningar sker genom att profilerna översänds och jämförs automatiskt (artikel 4.1). Sökningen ska göras i samband med brottsutredning och vara tillåten i den ansökande medlemsstaten. Om en träff uppkommer med en DNA-profil i ett register, ska referensuppgifterna för den aktuella profilen översändas utan dröjsmål (artikel 4.2 och artikel 11 i genomförandebeslutet).

I artiklarna 8 och 11 i genomförandebeslutet preciseras vilken information en begäran om automatisk jämförelse enligt artikel 4 och ett svar ska innehålla.

Andra bestämmelser om utbyte av DNA-uppgifter

När en automatisk sökning eller en automatisk jämförelse leder till en träff reglerar den anmodade medlemsstatens lagstiftning, inkluderande reglerna om rättslig hjälp, vilka personuppgifter och vilken ytterligare information som får översändas (artikel 5).

Varje medlemsstat ska utse ett nationellt kontaktställe för förmedlingen av uppgifter (artikel 6.1). Kontaktställets befogenheter regleras nationellt.

Insamling av DNA-prov och översändande av DNA-profiler

Om det i en stat pågår en brottsutredning eller ett straffrättsligt förfarande mot en person som vistas i en annan medlemsstat och om DNA-profil saknas för vederbörande, ska den medlemsstat där personen befinner sig under vissa förutsättningar på begäran ge en annan medlemsstat rättslig hjälp genom att ta ett DNA-prov från personen och analysera detta (artikel 7). Analysresultatet, DNA-profilen, ska översändas som en kombination av siffror och bokstäver till den ansökande medlemsstaten. Förutsättningarna för sådan rättslig hjälp är att den ansökande staten anger för vilket ändamål provtagning behövs, att det hade funnits förutsättningar för motsvarande åtgärd om personen i stället hade vistats i den staten, och att lagstiftningen i den anmodade staten tillåter insamling och analys av DNA-prov och översändande av DNA-profilen.

3.4.2 Fingeravtrycksuppgifter

Artiklarna 8–11 reglerar utbyte av uppgifter ur fingeravtrycksregister och automatiserad sökning i sådana register. I genomförandebeslutet preciseras principerna för utbyte av fingeravtrycksuppgifter (artikel 12), sökningskapaciteten (artikel 13) och

vad som ska gälla för begäran och svar angående fingeravtrycksuppgifter (artikel 14).

Automatisk sökning av fingeravtrycksuppgifter

Medlemsstaterna ska se till att referensuppgifter i nationella fingeravtrycksregister, bestående av fingeravtrycksuppgifter och en sifferbeteckning, hålls tillgängliga (artikel 8). Sifferbeteckningen ska bestå av en kombination av en kod som, vid överensstämmelse, gör det möjligt att hämta personuppgifter och ytterligare information från databaserna för vidarebefordran samt en kod för fingeravtrycksuppgifternas nationella ursprung (artikel 6 genomförandebeslutet). Referensuppgifterna får inte innehålla uppgifter som gör det möjligt att identifiera den berörda personen. Referensuppgifter som inte är kopplade till en viss person (s.k. oidentifierade fingeravtrycksuppgifter) ska kunna urskiljas som sådana.

Medlemsstaterna ska ge andra medlemsstaters kontaktställen tillträde till referensuppgifterna, dvs. fingeravtryck med tillhörande sifferuppgift (artikel 9). I enskilda fall, och enligt lagstiftningen i den ansökande medlemsstaten, ska utländska myndigheter tillåtas göra automatiska sökningar i registren (artikel 9.1). Kontaktställets förfrågan ska besvaras automatiskt (se definitionen i artikel 24). De tekniska detaljerna för sökförfarandet fastställs i artikel 12 och 13 i genomförandebeslutet.

Kontaktstället i den ansökande staten ska automatiskt sända referensuppgifter som kan bekräfta att de översända fingeravtrycksuppgifterna överensstämmer med en träff (artikel 9.2).

Översändande av övriga personuppgifter och ytterligare information

Om det vid en automatisk sökning konstateras att fingeravtrycken överensstämmer, regleras översändandet av övriga per-

sonuppgifter och ytterligare information av den anmodade medlemsstatens lagstiftning, inkluderande bestämmelser om rättslig hjälp (artikel 10).

Varje stat ska utse ett nationellt kontaktställe för förmedling av uppgifter (artikel 11.1). Dess befogenheter regleras nationellt.

3.4.3 Uppgifter ur fordonsregister

I *artikel 12* regleras utbyte av fordonsuppgifter. I syfte att förebygga och utreda brott, för undersökning av vissa överträdelser samt för att upprätthålla allmän säkerhet ska medlemsstaterna ge övriga medlemsstaters nationella kontaktställen tillgång till vissa uppgifter i de nationella fordonsregistren, med rätt att i enskilda fall göra automatiska sökningar (artikel 12.1). De uppgifter som omfattas är uppgifter om fordons ägare och innehavare samt om fordonet. Sökningarna ska ske genom angivande av fordonets fullständiga chassinummer eller registreringsnummer och vara tillåten enligt den ansökande medlemsstatens lagstiftning.

Varje stat ska utse ett nationellt kontaktställe för förmedling av uppgifter (artikel 12.2). Kontaktställets befogenheter regleras nationellt.

De tekniska förfarandereglerna fastställs i genomförandebeslutet. Principerna för automatisk sökning i fordonsregister regleras i artikel 15 i genomförandebeslutet. Där framgår bl.a. att medlemsstaterna ska använda en särskild version av programvaran för det europeiska informationssystemet avseende fordon och körkort (EUCARIS).

3.5 Samarbete vid större evenemang

Artiklarna 13–15 behandlar informationsutbyte i samband med större evenemang med gränsöverskridande verkningar. Som exempel på större evenemang nämns betydande idrottsevenemang och Europeiska rådets möten.

3.5.1 Översändande av andra uppgifter än personuppgifter

För att förebygga brott och upprätthålla allmän ordning och säkerhet i samband med större evenemang med gränsöverskridande verkningar, ska medlemsstaterna på begäran eller eget initiativ sända varandra nödvändiga, icke personrelaterade, uppgifter (artikel 13). Uppgiftsutbytet ska ske enligt den översändande medlemsstatens nationella lagstiftning.

Varje stat ska utse ett nationellt kontaktställe för förmedling av uppgifter (artikel 15). Dess befogenheter regleras nationellt.

3.5.2 Översändande av personuppgifter

För att förebygga brott och upprätthålla allmän ordning och säkerhet i samband med större evenemang med gränsöverskridande verkningar ska medlemsstaterna både på begäran och på eget initiativ sända varandra personuppgifter under vissa angivna förutsättningar (artikel 14.1). Utbytet av personuppgifter förutsätter att det – på grundval av lagakraftvunna domar eller andra fakta – finns skäl att anta att de personer som uppgifterna avser kommer att begå brott vid det berörda evenemanget eller att de utgör ett hot mot den allmänna ordningen och säkerheten. Utbytet ska vara tillåtet enligt lagstiftningen i den medlemsstat som sänder uppgifterna.

Översända personuppgifter får enbart behandlas för nyss angivna ändamål i samband med det aktuella evenemanget (artikel 14.2). När syftet med översändandet är uppnått, eller inte längre kan uppnås, ska uppgifterna utplånas. Uppgifterna ska alltid utplånas senast inom ett år.

Varje stat ska utse ett nationellt kontaktställe för förmedling av uppgifter (artikel 15). Dess befogenheter regleras nationellt.

3.6 Åtgärder för att förebygga terroristbrott

I syfte att förebygga terroristbrott får medlemsstaterna i enskilda fall, även utan föregående förfrågan, utbyta vissa personuppgifter i enlighet med nationell rätt. Detta regleras i *artikel 16*. De uppgifter som avses är efternamn, förnamn, födelsetid och födelseort samt uppgifter om varför det finns misstankar om att personen i fråga kommer att göra sig skyldig till terroristbrott (artikel 16.1 och 16.2). Uppgifterna får utbytas om det på grund av särskilda omständigheter finns anledning att anta att de personer som uppgifterna gäller kommer att göra sig skyldiga till sådana brott som avses i artiklarna 1–3 i terrorismrambeslutet[4].

Varje stat ska utse ett nationellt kontaktställe för förmedling av uppgifter (artikel 16.3). Dess befogenheter regleras nationellt.

Den översändande medlemsstaten får ställa upp villkor för hur de översända uppgifterna får användas (artikel 16.4). Sådana villkor är bindande för den mottagande medlemsstaten.

3.7 Andra former av samarbete

3.7.1 Gemensamma insatser

Gemensamma insatser behandlas i *artiklarna 17 och 19–23*. För att upprätthålla allmän ordning och säkerhet och förebygga brott samt för att fördjupa polissamarbetet får behöriga myndigheter i en medlemsstat inrätta gemensamma patruller och genomföra andra gemensamma insatser där tjänstemän från en eller flera medlemsstater deltar på en annan medlemsstats territorium (artikel 17.1).

Den medlemsstat där de gemensamma insatserna företas (värdstaten), får enligt sin lagstiftning och med den utsändande statens medgivande, ge andra medlemsstaters tjänstemän rätt att

[4] Rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism, EGT L 164, 22.6.2002, s. 3. Se även rådets rambeslut 2008/919/RIF av den 28 november 2008 om ändring av rambeslut 2002/475/RIF om bekämpande av terrorism, EUT L 330, 9.12.2008, s. 21.

utöva verkställande befogenheter (artikel 17.2). Befogenheterna får endast utövas under överinsyn av, och i regel i närvaro av, värdstatens tjänstemän. Samtliga tjänstemän lyder under värdstatens lagstiftning och värdstaten ansvarar för de utländska tjänstemännens handlingar. Dessa ska iaktta de anvisningar som meddelas av värdstatens myndigheter (artikel 17.3).

I artikel 19 fastställs vad tjänstemän som vid en gemensam insats vistas på en annan medlemsstats territorium får medföra och använda. Tjänstemännen får använda sin nationella tjänsteuniform. De får också inneha tjänstevapen, ammunition och annan utrustning enligt sin stats lagstiftning. Värdstaten kan emellertid förbjuda de utländska tjänstemännen att medföra vissa typer av tjänstevapen och viss ammunition eller utrustning (artikel 19.1). Vid all användning av tjänstevapen, ammunition och övrig utrustning ska värdstatens lagstiftning iakttas (artikel 19.2). Om en tjänsteman använder fordon på en annan medlemsstats territorium ska samma trafikregler gälla som för värdstatens tjänstemän (artikel 19.3).

Värdstaten är skyldig att skydda och bistå tjänstemän från andra medlemsstater på samma sätt som sina egna tjänstemän (artikel 20).

I artikel 21 regleras hur skadeståndsansvaret fördelas mellan värdstaten och tjänstemannens hemstat, om det uppstår skador i samband med insatsen.

Tjänstemän som verkar på annan medlemsstats territorium jämställs straffrättsligt med den andra statens tjänstemän (artikel 22). Detta gäller såväl i fråga om brott som tjänstemännen själva begår som brott som begås mot dem. Disciplinärt lyder tjänstemännen däremot under det egna landets lagstiftning (artikel 23).

3.7.2 Bistånd vid större evenemang, katastrofer och allvarliga olyckor

Medlemsstaterna ska enligt *artikel 18* på olika sätt bistå varandra vid större evenemang och liknande viktiga händelser, katastrofer

och allvarliga olyckor, i syfte att förhindra brott och upprätthålla allmän ordning och säkerhet. Biståndet ska bestå i att medlemsstaterna så tidigt som möjligt underrättar varandra om situationer som har gränsöverskridande verkningar och förmedlar väsentliga uppgifter som hänför sig till dem och i sådana situationer genomför och samordnar nödvändiga polisiära åtgärder inom sitt territorium. Biståndet kan även bestå i att tillhandahålla tjänstemän, specialister och rådgivare samt nödvändig utrustning.

3.8 Bestämmelser om dataskydd

I *artiklarna 24–32* finns bestämmelser om dataskydd och datasäkerhet.

3.8.1 Definitioner

I artikel 24.1 definieras vissa begrepp i rådsbeslutet.

Med ”behandling av personuppgifter” avses all behandling av personuppgifter eller en räcka av behandlingar med eller utan hjälp av automatiska förfaranden. Som exempel anges bl.a. insamling, registrering, lagring, bearbetning och spridning.

Med ”automatisk sökning” avses direkt tillgång till ett annat organs automatiska databas så att förfrågan besvaras fullständigt automatiskt.

”Förseende med en beteckning” innebär märkning av registrerade personuppgifter som inte syftar till att begränsa den framtida behandlingen av dem, till skillnad från ”spärrande” som är märkning i syfte att begränsa framtida behandling av personuppgifter.

3.8.2 Dataskyddsnivå

En lägsta dataskyddsnivå gäller för behandling av personuppgifter som översänds eller har översänts i enlighet med rådsbeslutet (artikel 25.1). Varje medlemsstat ska garantera att skyddet för sådana uppgifter motsvarar åtminstone den nivå som har fastställts i Europarådets konvention den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter och i tilläggsprotokollet den 8 november 2001. Rekommendation nr R (87) 15 den 17 september 1987 från Europarådets ministerkommitté till medlemsstaterna om polisens användning av personuppgifter ska också beaktas. Det sagda gäller även när uppgifterna inte behandlas automatiskt.

Uppgiftsutbytet med stöd av rådsbeslutet får inledas först när dataskyddsbestämmelserna har införlivats i nationell lagstiftning (artikel 25.2). Rådet beslutar enhälligt när denna förutsättning kan anses uppfylld. De medlemsstater som redan har inlett informationsutbytet inom ramen för Prümfördraget undantas från bestämmelsen (artikel 25.3).

3.8.3 Rätten att behandla uppgifter

Rätten att behandla personuppgifter är begränsad. Behandling får endast ske för de syften för vilka uppgifterna har översänts i enlighet med beslutet (artikel 26.1). Behandling för andra syften är tillåten endast om den medlemsstat som administrerar uppgifterna på förhand tillåter en sådan behandling och beslutet grundar sig på den mottagande medlemsstatens nationella lagstiftning. Tillstånd till annan behandling kräver vidare att lagstiftningen i den medlemsstat som administrerar uppgifterna medger behandling för sådana andra syften.

För behandling av uppgifter om DNA och fingeravtryck samt referensuppgifter som översänds genom det automatiska sökförfarandet gäller ytterligare restriktioner. Sådana uppgifter får behandlas endast för att fastställa om jämförda DNA-profiler

eller fingeravtrycksuppgifter överensstämmer eller för att utarbeta och lämna en begäran om rättslig hjälp samt för registrering (artikel 26.2). Den medlemsstat som administrerar registren får behandla uppgifter som har översänts endast om det är nödvändigt för att göra en jämförelse, svara på en automatisk sökning eller för registrering. När jämförelsen har avslutats, eller den automatiska sökningen har besvarats, ska uppgifterna omedelbart utplånas, om det inte är nödvändigt att behandla dem ytterligare för att utarbeta en begäran om rättslig hjälp eller för registrering.

Även för behandling av fordonsuppgifter som översänds genom det automatiska sökförfarandet gäller begränsningar. Den medlemsstat som administrerar uppgifterna får använda uppgifter som har översänts endast om det är nödvändigt för att besvara en automatisk sökning eller för registrering (artikel 26.3). När den automatiska sökningen har besvarats, ska de översända uppgifterna omedelbart utplånas, om det inte är nödvändigt med ytterligare behandling för registrering. Den sökande medlemsstaten får använda de uppgifter som har erhållits under sökningen endast för det förfarande som legat till grund för denna.

Kretsen av myndigheter som får hantera översända uppgifter begränsas till brottsbekämpande eller brottsbeivrande myndigheter samt de organ som administrerar registren (artikel 27). Översända uppgifter får lämnas vidare till andra myndigheter endast med tillstånd på förhand från den översändande myndigheten.

3.8.4 Uppgifternas korrekthet, aktualitet och lagringstid

Medlemsstaterna ska säkerställa att personuppgifterna är korrekta och aktuella (artikel 28.1). Om det visar sig att felaktiga uppgifter eller sådana uppgifter som inte borde ha översänts har sänts, ska den eller de medlemsstater som har mottagit uppgifterna underrättas om detta. Uppgifterna ska då *rättas* eller *utplånas* av mottagaren. Även i övrigt ska översända personuppgifter

rättas om det framgår att de är felaktiga. Den mottagande myndigheten är skyldig att underrätta den översändande myndigheten om att det finns skäl att anta att uppgifterna är felaktiga eller bör utplånas.

Uppgifter som enligt berörd person inte är korrekta, och vars korrekthet eller felaktighet inte kan fastställas, ska på dennes begäran *märkas* i enlighet med nationell lagstiftning (artikel 28.2). Märkningen får avlägsnas endast med den berörda personens medgivande eller genom beslut av en behörig domstol eller en oberoende dataskyddsmyndighet.

Översända personuppgifter ska *utplånas* om de inte borde ha översänts eller mottagits (artikel 28.3). Även personuppgifter som har översänts och mottagits korrekt ska utplånas om uppgifterna aldrig varit eller inte längre är nödvändiga för det syfte för vilket de översändes (artikel 28.3.a). Korrekt översända och mottagna uppgifter ska också utplånas sedan den tidsfrist som fastställts för lagring av uppgifterna enligt den översändande medlemsstatens nationella rätt har löpt ut. Detta förutsätter dock att den översändande myndigheten i samband med uppgiftsutbytet har informerat den mottagande myndigheten om lagringstiden (artikel 28.3.b). Om det finns skäl att anta att den berörda personens intressen skulle skadas om uppgifterna utplånas ska uppgifterna i stället *spärras* i enlighet med nationell rätt. Spärrade uppgifter får endast översändas eller användas i det syfte som ledde till att utplåningen förhindrades.

3.8.5 Dataskydd och datasäkerhet

Personuppgifterna ska skyddas mot oavsiktlig eller otillåten utplåning, oavsiktlig förlust, obehörig tillgång, obehörig eller oavsiktlig ändring och obehörigt offentliggörande (artikel 29.1). De närmare reglerna i genomförandebeslutet ska garantera att den senaste tekniken används för att säkerställa dataskydd och datasäkerhet, särskilt uppgifternas konfidentialitet och integritet (artikel 29.2). Godkända metoder för kryptering och autentise-

ring ska användas när allmänt tillgängliga kommunikationsnät utnyttjas.

3.8.6 Bestämmelser om registrering, dokumentation m.m.

I rådsbeslutet finns särskilda bestämmelser om registrering och dokumentation av översända och mottagna uppgifter både i fråga om automatiskt och icke-automatiskt översändande (artikel 30).

Artikel 30.1 behandlar registrering av icke-automatiskt översändande och mottagande av personuppgifter. Varje medlemsstat ska garantera att översändning och mottagande registreras hos den myndighet som administrerar databasen och hos den sökande myndigheten för kontroll av att sändningen är tillåten. Registreringen ska omfatta skälet till översändandet, de översända uppgifterna, datum för översändandet samt namn eller beteckning på den myndighet som genomför sökningen och den myndighet som administrerar databasen.

En automatisk sökning eller jämförelse får genomföras endast av de tjänstemän vid nationella kontaktställen som särskilt har bemyndigats att göra detta (artikel 30.2). En förteckning över dessa tjänstemän ska på begäran lämnas till dataskyddsmyndigheterna och de övriga medlemsstaterna. Även för automatiska sökningar gäller att varje översändande och mottagande ska registreras, tillsammans med uppgift om huruvida sökningen har lett till träff eller inte, av den myndighet som administrerar databasen och av den sökande. Registreringen ska omfatta översända uppgifter, datum och tidpunkt för översändandet samt namn eller beteckning på den myndighet som genomför sökningen och den myndighet som administrerar databasen. Den sökande myndigheten ska dessutom registrera syftet med sökningen eller översändandet samt vilken tjänsteman som initierade förfarandet (artikel 30.2.b).

Den registreringskyldiga myndigheten ska på begäran, utan dröjsmål och senast inom fyra veckor, delge den berörda medlemsstatens dataskyddsmyndigheter de registrerade uppgifterna

(artikel 30.3). Uppgifterna får endast användas för övervakning av dataskyddet och för att garantera datasäkerheten. De ska lagras i två år och därefter utplånas (artikel 30.4).

Artikel 30.5 reglerar kontrollen över informationsutbytet. Den ska utövas av oberoende dataskyddsmyndigheter eller de rättsliga myndigheterna i respektive medlemsstat. Var och en kan hos dessa myndigheter ansöka om en granskning av lagligheten av behandlingen av sina personuppgifter enligt nationell rätt. De registreringsskyldiga ska göra stickprov och kontrollera översändningarnas laglighet. Resultaten av kontrollerna ska för granskningsändamål förvaras i 18 månader, varefter de ska utplånas.

En dataskyddsmyndighet kan av en annan medlemsstats dataskyddsmyndighet anmodas att genomföra nödvändiga inspektioner för kontroll av den personuppgiftsbehandling som sker med stöd av rådsbeslutet. Kontrollmyndighetens befogenheter regleras nationellt. Myndigheterna ska utföra de inspektioner som är nödvändiga för det ömsesidiga samarbetet.

3.8.7 Rätten till information och skadestånd

På begäran ska en person, enligt nationell rätt, få information om de uppgifter om honom eller henne som har varit föremål för behandling (artikel 31.1). Informationen ska lämnas utan oskäliga avgifter, i en förståelig form och utan dröjsmål. Den ska även innehålla uppgifternas ursprung, mottagare eller kategori av mottagare, det avsedda ändamålet med behandlingen och, när så krävs i nationell lagstiftning, dess rättsliga grund. Den berörda personen ska också ha rätt att kräva att felaktiga uppgifter korrigeras och att uppgifter som behandlats på ett otillbörligt sätt utplånas. Personer, vars dataskyddsrättigheter har kränkts, ska ha möjlighet att överklaga hos en oavhängig domstol eller hos en oberoende tillsynsmyndighet och kräva skadestånd eller annan ersättning (artikel 31.1). Förfarandet ska följa nationell rätt i den medlemsstat där personen hävdar sina rättigheter.

När en myndighet i en medlemsstat har översänt personuppgifter med stöd av rådsbeslutet, kan den mottagande myndigheten i en annan medlemsstat inte hänvisa till att de översända uppgifterna var felaktiga för att undgå sitt ansvar mot den skadelidande (artikel 31.2). Om en mottagande myndighet döms att betala skadestånd till följd av att den har använt felaktigt översända uppgifter ska den översändande myndigheten ersätta denna.

En mottagande stat ska på begäran informera översändande stat om behandlingen av de översända uppgifterna och de resultat som har erhållits (artikel 32).

3.9 Genomförande och slutbestämmelser

Artiklarna 33–37 innehåller bestämmelser om genomförandet av rådsbeslutet.

Varje medlemsstat ansvarar själv för de driftskostnader som dess egna myndigheter ådrar sig i samband med tillämpningen av rådsbeslutet (artikel 34).

I artikel 35 redovisas hur rådsbeslutet förhåller sig till andra internationella överenskommelser. De medlemsstater som har ratificerat Prümfördraget ska tillämpa rådsbeslutet i stället för fördragets bestämmelser.

Medlemsstaterna ska genomföra beslutet inom ett år från det att beslutet har trätt i kraft (artikel 36.1), med undantag för bestämmelserna om automatisk sökning och jämförelse i register, där medlemsstaterna ges tre år för att vidta nödvändiga åtgärder.

Rådsbeslutet trädde i kraft tjugo dagar efter offentliggörandet i Europeiska unionens officiella tidning (artikel 37). Rådsbeslutet publicerades den 6 augusti 2008 och gäller därmed från den 26 augusti 2008. Det innebär att de obligatoriska delarna av beslutet till stora delar ska vara genomförda den 26 augusti 2009.

4 Andra EU-initiativ om polisiärt samarbete och informationsutbyte

4.1 Den allmänna utvecklingen

Prümrådsbeslutet är avsett att komplettera det etablerade och väl fungerande polisiära samarbetet inom Europeiska unionen. I takt med den ökade rörligheten över gränserna, avskaffandet av gränskontroller och den allmänna internationaliseringen växer ständigt behovet av att finna nya samarbetsformer. En särskilt viktig drivkraft för att utveckla det polisiära samarbetet, bl.a. rörande gränsöverskridande informationsutbyte, är det ökade behovet av skydd mot terroristattacker och annan grov brottslighet. Efter terroristattackerna i USA 2001, i Madrid 2004 och i London 2005 har ett ökat informationsutbyte konstaterats vara av central betydelse för det brottsbekämpande samarbetet. Ett flertal rättsakter har antagits med detta i fokus (se avsnitt 4.2).

Vidare är det s.k. Haagprogrammet för stärkt frihet, säkerhet och rättvisa i Europeiska unionen, som antogs av Europeiska rådet i november 2004, av grundläggande betydelse för det polisiära samarbetet. Prümrådsbeslutet refererar till detta i preambeln (se avsnitt 3.2). I Haagprogrammet slogs fast att informationsutbytet efter den 1 januari 2008 bör styras av en s.k. tillgänglighetsprincip. Den innebär att en tjänsteman vid en brottsbekämpande myndighet i en medlemsstat ska göra befintlig information tillgänglig för en motsvarande tjänsteman i en annan stat som behöver informationen för att utföra sina uppgifter. I

programmet konstateras också att metoderna för informationsutbyte bör bygga på användning av ny teknik och anpassas till varje typ av information, i förekommande fall genom ömsesidig tillgång till eller kompatibilitet med nationella databaser eller i annat fall genom direkt tillgång till befintliga centrala databaser i Europeiska unionen. Nya centraliserade europeiska databaser bör, enligt vad rådet uttalade, inrättas endast på grundval av studier som har visat deras mervärde.

Sedan Haagprogrammet beslutades har ett stort antal instrument som reglerar samarbetet mellan medlemsstaternas brottsbekämpande myndigheter vuxit fram. Flera rättsakter rör informationsutbyte och påverkar bl.a. medlemsstaternas personuppgiftsbehandling i olika avseenden. Samarbetet sker inom ramen för den s.k. tredje pelaren och är därmed mellanstatligt.[14]

4.2 Former för samarbete och informationsutbyte vid bekämpning och lagföring av brott

4.2.1 Europol

Det fördjupade gränsöverskridande polisiära samarbetet och utbytet av information påverkas i hög grad av utvecklingen av det polisiära samarbetet inom ramen för Europeiska unionens gemensamma polisbyrå, Europol. En av Europols viktigaste uppgifter är att samla in och bearbeta information om allvarlig gränsöverskridande brottslighet av visst slag och att förmedla denna information vidare till medlemsstaterna.

Europols verksamhet bygger på möjligheten att från medlemsstaterna hämta in och analysera underrättelseinformation

[14] Genom Lissabonfördraget den 13 december 2007 om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen ändras dock stora delar av den nuvarande primärrätten; bl.a. försvinner den nuvarande indelningen i tre olika pelare. Det straffrättsliga samarbetet och polissamarbetet kommer att bli föremål för gemensamt beslutsfattande (se vidare prop. 2007/08:168 s. 45 och 54 f.). Detta innebär bl.a. att beslutanderätten i dessa delar förs över till unionen och att medlemsstaternas genomförande av de gemensamma besluten kommer att omfattas av kommissionens kontrollbefogenheter.

om viss grov gränsöverskridande brottslighet och sedan återföra resultatet av analyserna till medlemsstaterna. För svenskt vidkommande tillämpas 7 § första stycket polisdatalagen (1998:622) vid informationsutbytet. Genom ett förslag till rådsbeslut i juni 2008, som ska ersätta Europolkonventionen och dess ändringsprotokoll, förändras den rättsliga grunden för Europols verksamhet från ett mellanstatligt samarbete till att Europol blir ett EU-organ. Europol ges bl.a. möjlighet att upprätta och driva nya system för informationsbehandling, t.ex. avseende terroristbekämpning. Utkastet till rådsbeslut innehåller bl.a. vissa nya bestämmelser om dataskydd, t.ex. inrättande av ett oberoende uppgiftsskyddsombud. Riksdagen har godkänt utkastet till rådsbeslut.[15] Rådsbeslutet är ännu inte antaget.

4.2.2 Eurojust

Åklagarsamarbetet inom Europeiska unionen bedrivs primärt inom ramen för Eurojust, som inrättades år 2002 och har status som EU-organ.[16] Eurojusts huvuduppgift är att främja och förbättra samordningen mellan medlemsstaternas brottsbekämpande myndigheter vid bekämpningen av grov gränsöverskridande brottslighet. I dess uppdrag ingår bl.a. att hjälpa medlemsstaterna i frågor om internationell rättslig hjälp och utlämning.

I Eurojust ingår en nationell medlem från varje stat. Om medlemmen har några rättsliga befogenheter i förhållande till sin hemstat avgörs av den staten.

Eurojust kan uppmana rättsliga myndigheter i en medlemsstat som berörs av ett ärende att genomföra brottsutredning och väcka åtal och kan vidare anmana berörda myndigheter att samordna utredningar. Eurojust saknar emellertid egna rättsliga be-

[15] Prop. 2008/09:14, bet. 2008/09:JuU6, rskr. 2008/09:63.
[16] Se rådets beslut 2002/187/RIF av den 28 februari 2002 om inrättande av Eurojust för att stärka kampen mot grov brottslighet och rådets beslut 2003/659/RIF av den 18 juni 2003 om ändring av beslut 2002/187/RIF om inrättande av Eurojust för att stärka kampen mot grov brottslighet, EGT L 63, 6.3.2002, s. 1 och EUT L 245, 29.9.2003, s. 44.

fogenheter. Beslut i brottsutredningar fattas alltid på nationell nivå och med tillämpning av nationell lagstiftning.

4.2.3 European Judicial Network

European Judicial Network (EJN) inrättades år 1998 efter beslut av Europeiska rådet.[17] Nätverket består av företrädare för nationella myndigheter (kontaktpunkter) som arbetar med internationellt straffrättsligt samarbete. Kontaktpunkterna är aktiva mellanhänder för att underlätta det rättsliga samarbetet mellan medlemsstaterna, framför allt när det gäller att bekämpa grov brottslighet. Kontaktpunkterna har dagliga kontakter, vanligtvis per telefon eller e-post, i konkreta brottsutredningar. Dessutom träffas de ett antal gånger per år för att utbyta erfarenheter och diskutera praktiska och rättsliga problem.

För att effektivisera det rättsliga nätverket och tydliggöra fördelningen av ärenden mellan Eurojust och nätverket har ett nytt rådsbeslut antagits som ersätter rådsbeslutet från år 1998.[18]

4.2.4 Det svenska initiativet

Den tillgänglighetsprincip som är väsentlig i Europeiska unionens arbete för att utveckla informationsutbytet är en av grundstenarna i rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater. Rambeslutet, som kom till efter ett svenskt initiativ, innebär att brottsbekämpande myndigheter i medlemsstaterna redan på underrättelsestadiet, och över myndighetsgränserna, snabbt ska kunna utbyta befintlig information och befintliga underrättelser. Genom rambeslutet åtar sig medlemsstaterna

[17] EGT L 191, 7.7.1998, s. 4.
[18] Rådets beslut 2008/976/RIF av den 16 december 2008 om det europeiska rättsliga nätverket, EUT L 348, 24.12.2008, s. 130.

bl.a. att dels lämna viss information på begäran av annan stat, dels spontant lämna vissa uppgifter. Medlemsstaterna ska ha genomfört bestämmelserna i rambeslutet senast den 19 december 2008. I en departementspromemoria, som innehåller en bedömning av vilka författningsändringar som behövs för att genomföra rambeslutet i svensk rätt, föreslogs en ny förordning i anledning av samarbetet.[19] Den nya förordningen trädde i kraft den 1 februari 2009.[20]

4.2.5 Utbyte av uppgifter i kriminalregister

Uppgifter om brottmålsdomar utbyts i dag med stöd av 1959 års europeiska konvention om ömsesidig rättslig hjälp i brottmål. Systemet har visat sig ha betydande brister och domstolar meddelar ofta dom enbart med beaktande av tidigare domar som finns upptagna i deras nationella register, men utan kunskap om eventuella domar i andra medlemsstaters register. För att förbättra och underlätta informationsutbytet mellan Europeiska unionens medlemsstater presenterade kommissionen därför i december 2005 ett förslag till rådets rambeslut om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll.[21] I utkastet till rambeslut föreslås att varje medlemsstat som meddelar en dom mot en medborgare i en annan medlemsstat ska informera medborgarstaten om domen. Medborgarstaten ska därefter lagra informationen. Utkastet till rambeslut lägger också bl.a. grunden för nästa steg i arbetet med att effektivisera informationsutbytet och möjliggöra elektronisk uppgiftsöverföring.[22] Riksdagen har godkänt utkastet till rambeslut.[23] Rambeslutet är ännu inte antaget.

---

[19] Se Ds 2008:72.

[20] Förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen.

[21] KOM (2005) 690 slutlig.

[22] Ett datoriserat system för utbyte av uppgifter i kriminalregistret föreslås komma till stånd genom inrättandet av ett europeiskt informationssystem för utbyte av uppgifter ur kriminalregister (Ecris), se vidare förslag till rådets beslut om inrättande av Europeiska

4.2.6 Schengens informationssystem

Information utbyts också genom Schengens informationssystem (SIS). SIS har tillkommit genom Schengenkonventionen. Denna innehåller bestämmelser om praktiska åtgärder för att uppnå Schengenavtalets syfte. Bestämmelserna gäller bl.a. polissamarbete, rättsligt samarbete, dataskydd, samarbete om narkotikabekämpning, harmoniserad viseringspolitik och enhetliga yttre gränskontroller. SIS, som är ett datasystem som fungerar som ett efterlysningshjälpmedel, och i viss mån även som ett spaningshjälpmedel, utgör en del av Schengensamarbetet. SIS är nu föremål för förändring inom ramen för ”den andra generationen av SIS”, benämnd SIS II. Datasystemet SIS II är, i likhet med SIS, främst ett efterlysnings- och spaningsregister som till exempel gör det möjligt för polisen att efterlysa brottslingar och försvunna personer inom Schengenområdet. Förutom tekniska förändringar innebär SIS II bl.a. att nya kategorier av uppgifter ska kunna registreras i syfte att effektivisera brottsbekämpningen. Dessutom kommer kontrollen av att registrerade uppgifter används på föreskrivet sätt att bli effektivare, vilket stärker skyddet för enskildas personliga integritet. Det nuvarande systemet anses vara tekniskt föråldrat och klarar inte kommande behov.[24]

I SIS kan varje Schengenstat föra in uppgifter om personer samt om fordon eller andra föremål som är efterlysta eller på annat sätt eftersökta. Denna stat kan samtidigt begära att en viss åtgärd ska vidtas om personen eller föremålet påträffas vid en gränskontroll eller i en annan Schengenstat. I varje Schengenstat finns ett s.k. Sirenekontor som ansvarar för registreringarna i SIS och lämnar viss kompletterande information till varandra.

informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris) i enlighet med rambeslut 2008/XX/RIF, KOM (2008) 332 slutlig.

[23] Se prop. 2008/09:18, bet. 2008/09:JuU11, rskr. 2008/09:33.

[24] Se vidare prop. 2006/07:33, bet. 2006/07:JuU3, rskr. 2006/07:95 och Ds 2008:81.

4.2.7 VIS

Utvecklingen av uppgiftsutbytet mellan medlemsstaterna rör också bl.a. viseringsområdet. År 2004 inrättades informationssystemet för viseringar (VIS) som ett system för utbyte av viseringsuppgifter mellan medlemsstaterna.[25] Samma år presenterade kommissionen ett förslag till förordning om VIS och utbytet av uppgifter mellan medlemsstaterna om viseringar för kortare vistelser (VIS-förordningen). Europaparlamentet och rådet har nu gemensamt antagit ett reviderat förslag till VIS-förordning.[26] VIS-förordningen kompletteras av ett tredjepelarbeslut i form av ett beslut av rådet.[27] Enligt detta rådsbeslut ska särskilt utsedda brottsbekämpande myndigheter i medlemsstaterna samt Europol under vissa förutsättningar ges tillgång till uppgifter ur VIS i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott. Reglerna för hur myndigheterna får använda registret är restriktiva och uppgifter får endast lämnas ut under vissa speciella förutsättningar. Ett grundläggande krav för att en brottsbekämpande myndighet ska få tillgång till uppgifter i VIS är att den lämnar en motiverad, skriftlig eller elektronisk, begäran till en central åtkomstpunkt som ska kontrollera att samtliga villkor för tillgång till VIS är uppfyllda. Vidare krävs bl.a. att sökningarna är nödvändiga för att förebygga, upptäcka eller utreda terroristbrott eller andra grova brott, att sökningarna krävs i ett specifikt ärende och att det finns rimliga skäl att anse att inhämtandet av VIS-uppgifter väsentligen kommer att bidra till att brotten i fråga förebyggs, upptäcks eller utreds.

---

[25] Rådets beslut 2004/512/EG om inrättande av Informationssystemet för viseringar (VIS), EUT L 213, 15.6.2004, s. 5.

[26] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse, EUT L 218, 13.8.2008, s. 60.

[27] Rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott, EUT L 218, 13.8.2008, s. 129.

Regeringen har på ett övergripande plan övervägt vilka lagändringar som kan bli nödvändiga med anledning av rådsbeslutet. Riksdagen har godkänt utkastet till rådsbeslut.[28]

4.3 Dataskyddsrambeslutet

Det stora antalet nya EU-instrument rörande utvidgat polisiärt och rättsligt samarbete avseende gränsöverskridande informationsutbyte har föranlett ett rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (det s.k. dataskyddsrambeslutet). Dataskyddsrambeslutet förpliktar medlemsstaterna att behandla uppgifter som utbyts mellan staterna inom ramen för det angivna samarbetet på sådant sätt att skyddet för enskildas integritet värnas. Det innehåller bestämmelser som avser att förstärka skyddet vid behandling av personuppgifter som överförs. Rambeslutet utgör ett komplement till andra instrument om informationsutbyte inom ramen för polisiärt och straffrättsligt samarbete. Det innehåller bl.a. bestämmelser om allmänna utgångspunkter för behandlingen av personuppgifter och känsliga personuppgifter, rättelse, radering och gallring av personuppgifter, information till den registrerade samt skadestånd och sanktioner. Till stora delar motsvarar innehållet dataskyddsdirektivet, som i svensk rätt har genomförts i personuppgiftslagen (se vidare avsnitten 6.2.5 och 6.3.1). Vidare finns bl.a. särskilda bestämmelser som begränsar möjligheterna att behandla utbytta personuppgifter.

Regeringen har på ett övergripande plan övervägt vilka lagändringar som kan bli nödvändiga med anledning av det utkast till rådsbeslut som lagts fram. Riksdagen har godkänt utkastet till rambeslut,[29] som nu också har antagits av rådet.[30]

---

[28] Prop. 2007/08:132, bet. 2007/08:JuU27, rskr. 2007/08:250.
[29] Prop. 2008/09:16, bet. 2008/09:JuU7, rskr. 2008/09:41.
[30] Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, EUT L 350, 30.12.2008, s. 60.

4.4 Eurodac

Ett system för att identifiera asylsökande inrättades i januari 2003. För detta ändamål finns en europeisk databas med fingeravtryck, Eurodac.[31] Som en del av ett rutinförfarande vid begäran om asyl tas fingeravtryck på alla sökande över 14 år. Fingeravtrycken skickas i digital form till en central enhet vid Europeiska kommissionen, där de automatiskt jämförs med andra avtryck som lagrats i databasen. När en medlemsstat skickar en uppsättning fingeravtryck till Eurodac får den genast besked om dessa stämmer överens med andra fingeravtryck som redan finns i databasen. Om så är fallet, kan staten välja att skicka tillbaka personen till det land dit han eller hon först kom eller där personen först ansökte om asyl. Myndigheterna i denna stat ansvarar då för att fatta beslut om den sökandes rätt att stanna. Om fingeravtrycken inte förekommer i databasen, handlägger den stat som skickat in fingeravtrycken ärendet.

Den europeiske datatillsynsmannen (EDPS) utövar tillsyn över behandlingen av personuppgifter i den centrala databasen. De nationella dataskyddsmyndigheterna utövar tillsyn över nationell hantering av Eurodac-uppgifter och överföringen av uppgifter till den centrala databasen.

[31] Rådets förordning (EG) nr 2725/2000 av den 11 december 2000 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av Dublinkonventionen, EGT L 316, 15.12.2000, s. 6.

5 Nationella register som berörs av Prümrådsbeslutet

5.1 Allmänna utgångspunkter

I avsnitt 3 har närmare beskrivits hur Prümrådsbeslutet ger utländska myndigheter möjligheter att söka i svenska register med DNA-, fingeravtrycks- och fordonsuppgifter, men också ger svenska myndigheter möjlighet att utföra motsvarande sökningar och ta emot och jämföra uppgifter som med stöd av rådsbeslutet överförs från en annan medlemsstat. Det är mot den bakgrunden angeläget att redovisa nuvarande ordning när det gäller provtagning, analys och registrering i de svenska registren. Avsnitt 5.2 behandlar provtagning, analys och registrering av DNA. I avsnitt 5.3 beskrivs på motsvarande sätt fingeravtryck. Sist redovisas vad som gäller för vägtrafikregistret (avsnitt 5.4).

5.2 DNA-register

5.2.1 Provtagning

Prov för DNA-analys kan tas bl.a. genom salivprov, blodprov eller hårprov. Att ta DNA-prov i form av salivprov eller blodprov för DNA-analys i samband med en brottsutredning förutsätter i princip ett beslut om kroppsbesiktning enligt 28 kap. rättegångsbalken (28 kap. 12, 12 a och b §§ rättegångsbalken). Med kroppsbesiktning avses en undersökning av människokroppens yttre och inre samt tagande av prov från människokroppen

och undersökning av sådana prov (28 kap. 12 § rättegångsbalken).

För andra prov än salivprov tillämpas 28 kap. 12 § rättegångsbalken. Den som är skäligen misstänkt för ett brott på vilket fängelse kan följa får kroppsbesiktigas bl.a. för att utröna omständigheter som kan vara av betydelse för utredning om brottet. I samband med det kan DNA-prov tas. Förutsättningarna är att provet behövs för att klarlägga den misstänktes del i brottet. Analysen av provet kan givetvis även fria från misstanke.

Med stöd av 28 kap. 12 a § rättegångsbalken får salivprov tas från den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa. Syftet med provtagning enligt denna bestämmelse är att göra en DNA-analys av provet och registrera uppgifter om resultatet av analysen i det utredningsregister eller det DNA-register som förs med stöd av polisdatalagen (prop. 2005/06:29 s. 39). Sådana prov får, till skillnad mot prov som tas med stöd av den allmänna regeln i 28 kap. 12 § rättegångsbalken, tas även om det inte behövs för utredningen av det aktuella brottet. Om den misstänkte redan finns i DNA-registret eller om prov redan har tagits under utredningen av brottet, bör någon ny provtagning inte ske. Övriga bestämmelser i 28 kap. rättegångsbalken om kroppsbesiktning är tillämpliga. Således är proportionalitetsprincipen i 3 a § tillämplig, vilket innebär att det vid varje enskilt provtagningstillfälle ska övervägas om åtgärden är proportionerlig (prop. 2005/06:29 s. 39). Det är därför t.ex. knappast aktuellt att ta DNA-prov i de fall där det brott som misstanken avser ter sig så bagatellartat att påföljden kan antas komma att stanna vid böter.

Enligt 28 kap. 12 b § första stycket rättegångsbalken får salivprov också tas från personer som inte är misstänkta för brott eller där misstanken ligger på en lägre nivå än skälig misstanke. Förutsättningarna för att få ta ett sådant prov är att dels att syftet är att underlätta identifiering vid utredning av brott på vilket fängelse kan följa, dels att det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet. Begreppet ”synnerlig anledning” tolkas i praxis så att det ska föreligga fak-

tiska omständigheter som påtagligt visar att man med fog kan förvänta sig att uppnå det avsedda resultatet med åtgärden (SOU 1995:47 s. 298). Det är således inte tillåtet att slentrianmässigt besluta om kroppsbesiktning av en stor mängd personer. I de fall där DNA-prov har tagits från någon som inte är skäligen misstänkt får analysresultatet inte jämföras med uppgifter i DNA-register. Provresultatet får inte heller i övrigt användas för något annat ändamål än det för vilket det togs.

Enligt 36 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare och 28 kap. 12 b § tredje stycket rättegångsbalken får DNA-prov inte tas på den som är under 15 år.

5.2.2 Analys och registrering

DNA-registren

När polisregisterlagstiftningen ändrades år 1999 infördes regler om DNA-register (prop. 1997/98:97, bet. 1997/98:JuU20). Samtidigt inrättades två register, DNA-registret och spårregistret, medan utredningsregistret tillkom när möjligheterna till provtagning utvidgades år 2006 (prop. 2005/06:29, bet. 2005/06:JuU7). Reglerna om DNA-register placerades i polisdatalagen för att ge polisen möjlighet att utnyttja DNA-tekniken redan på spaningsstadiet, innan misstankar kunnat riktas mot en viss person, och för att kunna jämföra spåranalyser t.ex. från en brottsplats med DNA-profilerna i registret (prop. 1997/98:97 s. 133 f.).

Uppgifter om resultat av DNA-analyser får behandlas endast för att underlätta identifiering av personer i samband med utredning av brott. Med stöd av 22 § polisdatalagen för Rikspolisstyrelsen ett DNA-register, ett utredningsregister och ett spårregister.

DNA-registret innehåller uppgifter om resultatet av DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som genom lagakraftvunnen dom har dömts till annan påföljd än böter eller har god-

känt ett strafföreläggande som avser villkorlig dom (23 § polisdatalagen). Registreringen av analysresultat ska begränsas till uppgifter som ger information om den registrerades identitet. Resultat som kan ge upplysning om personliga egenskaper får inte registreras (24 § första stycket polisdatalagen). DNA-registret får utöver ovanstående uppgifter endast innehålla upplysning om i vilket ärende analysen har gjorts och vem analysen avser (24 § andra stycket polisdatalagen).

Utredningsregistret omfattar personer som är skäligen misstänkta för brott på vilket fängelse kan följa (24 a § polisdatalagen). Samma regler gäller för registrering av uppgifter i utredningsregistret som för DNA-registret.

Spårregistret innehåller uppgifter om DNA-analyser som har gjorts under utredning av brott och som inte kan hänföras till en identifierbar person. Uppgifterna som registreras avser spår från en brottsplats eller från en målsägandes kläder eller kropp, om man inte kan utröna vem som har avsatt spåret. En uppgift som har förts in i spårregistret ska tas bort så snart det finns information som visar vem det analyserade spåret härrör från (prop. 1997/98:97 s. 140). Utöver uppgifter om analysresultat får detta register enbart innehålla upplysningar som visar i vilket ärende analysen har gjorts (25 § polisdatalagen). Analysresultat från DNA-prov får i vissa fall jämföras med uppgifter i spårregistret (26 § polisdatalagen). Om analysresultatet är ett ”spår”, dvs. tillhör en oidentifierad person, får för det första en jämförelse göras med andra analysresultatet i spårregistret. Om resultatet däremot avser en identifierad person får en jämförelse endast ske med uppgifter i DNA-registret eller om personen är skäligen misstänkt för brott.

Enligt 11 § polisdataförordningen får Statens kriminaltekniska laboratorium (SKL), polismyndigheter och åklagarmyndigheter ha direktåtkomst till DNA-registret, utredningsregistret och spårregistret.

Bestämmelserna om innehållet i registren och regleringen i övrigt ändras inte enligt det förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet som för

närvarande bereds inom Regeringskansliet (Ds 2007:43 s. 279 f. och s. 460 f.).

Analys, registrering och träffrapport

SKL analyserar DNA-prov och tar fram en DNA-profil som registreras samt jämförs med andra DNA-profiler.

Vid en kriminalteknisk DNA-analys undersöks en liten del av arvsmassan med inriktning på olika analyser av vad som benämns STR-områden (Short Tandem Repeats). Typbestämningen av ett antal sådana STR-områden presenteras som en sifferkombination, en DNA-profil. DNA-profilen utgör alltså resultatet av DNA-analysen.

I DNA-registren får enbart resultatet av sådana DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken tas in. Det betyder bl.a. att resultatet av DNA-prov som har tagits med stöd av samtycke inte får registreras i vare sig DNA-registret eller utredningsregistret (23 och 24 a §§ polisdatalagen samt prop. 2005/06:29 s. 31).

Registreringen av ett analysresultat ska begränsas till uppgifter som ger information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får, som tidigare nämnts, inte registreras (24 § polisdatalagen). I praktiken innebär det att enbart en sifferkombination registreras och används för jämförelse med andra registreringar.[32] Den del av DNA:t som typbestäms hör till den ickekodifierade delen av DNA:t. Det finns därför inga personliga egenskaper kopplade till dessa. Uppgifter om kön registreras inte i dag.

För närvarande är cirka 50 000 personer registrerade i de svenska DNA-registren. Rikspolisstyrelsen har emellertid pekat på att antalet registrerade personer i framtiden kan bli minst det dubbla.

[32] Rikspolisstyrelsen, Polisens användning av salivprov för DNA-analys, Inspektionsrapport 2008:1, s. 9.

Inom ett ärende jämförs först de framtagna DNA-profilerna mot varandra. Det innebär att spår från en brottsplats och en misstänkt gärningsman jämförs mot varandra. Om dessa stämmer överens behöver DNA-profilerna från brottsplatsspåren inte läggas in i spårregistret, eftersom de har knutits till en person. Kan resultatet däremot inte hänföras till en identifierbar person läggs DNA-profilerna in i spårregistret.

DNA-profilerna i spårregistret jämförs regelbundet med registrerade DNA-profiler i utrednings- och DNA-registret. Vid en automatisk jämförelse mellan DNA-profiler i de olika registren redovisas resultatet i en träffrapport. En träffrapport kan innehålla en eller flera träffar mellan DNA-profiler från de olika registren. Det anges inte i vilket av registren DNA-profilerna finns. Varje träff har ett unikt "träff ID" och är SKL:s interna löpnummer på träffen. Det finns ingen "träffhistorik" eftersom spåren alltid gallras vid träff mot en person.

Ett *sökprov* utgörs av den DNA-profil som är senast registrerad. Per träffrapport redovisas ett sådant sökprov. Detta prov kan komma från en person eller ett spår. *Träffprov* är den eller de DNA-profiler som finns registrerade sedan tidigare och som vid sökning träffar mot en ny DNA-profil som registrerats, dvs. sökprovet. Träffprovet kan komma från en person eller ett spår.

En *registerträff* består av en kombination av ett sökprov och ett träffprov som har en gemensam DNA-profil. Den gemensamma DNA-profilen för sök- och träffprov är underlaget för den statistiska beräkningen av risken för slumpmässig överensstämmelse, vilket i sin tur utgör underlaget för slutsatsen om DNA-uppgifterna stämmer överens.

Gallring

Uppgifter i *DNA-registret* ska gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen om belastningsregister (27 § första stycket polisdatalagen). Detta innebär för en icke-frihetsberövande påföljd tio år efter det att

dom har meddelats och vid frihetsberövande påföljd tio år efter det att påföljden har verkställts. Om nya domar tillkommer under tiden förlängs gallringsfristen. Har en DNA-profil registrerats efter den 1 januari 2006 görs en kontroll mot misstankeregistret innan gallring sker. Skulle personen vara registrerad i misstankeregistret flyttas DNA-profilen från DNA-registret till utredningsregistret.

I *utredningsregistret* ska DNA-profilen gallras senast när den registrerade personen döms till annan påföljd än böter. Uppgifterna förs då i stället över till DNA-registret. Uppgiften gallras om förundersökning eller åtal läggs ner, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade godkänner ett strafföreläggande som avser enbart böter (27 § andra stycket polisdatalagen).

Som framgått ovan gallras inte uppgifterna i DNA-registret och utredningsregistret om det finns en anteckning om personen i belastnings- eller misstankeregistret. Anteckningen måste gälla ett brott som i sig medger registrering i DNA-registret, men den behöver inte avse det brott som föranledde provtagningen. För att uppgifterna ska ligga kvar i utredningsregistret måste en ny misstanke dels ha registrerats i misstankeregistret innan den misstanke som föranledde registreringen har avförts, dels gälla ett brott på vilket fängelse kan följa. Hanteringen sker automatiskt eftersom DNA-registret och utredningsregistret har förbindelse med belastningsregistret och misstankeregistret.[33]

Spår från brottsplatser i form av DNA-profiler gallras (raderas) från *spårregistret* när träff uppkommer mot en person, dvs. när man vet från vem spåret härrör. I övriga fall gallras DNA-profilerna senast 30 år efter registreringen (27 § tredje stycket polisdatalagen). SKL ska underrättas av den polismyndighet som skickade in spåret för analys när brottet är uppklarat eller provet är irrelevant.

[33] Se vidare Rikspolisstyrelsen, Polisens användning av salivprov för DNA-analys, Inspektionsrapport 2008:1, s. 9.

5.3 Fingeravtrycksregister

5.3.1 Tagande av fingeravtryck

Fingeravtryck, som avsätts av papillarlinjemönstret, utgörs i princip av naturliga utsöndringsprodukter från olika körtlar i kroppen och föroreningar från omgivningen. Enligt 28 kap. 14 § rättegångsbalken samt förordningen (1992:824) om fingeravtryck m.m. ska fingeravtryck och fotografi alltid tas av den som häktats. I vissa uppräknade fall ska fingeravtryck också tas av den som är anhållen. Enligt 2 § andra stycket förordningen om fingeravtryck m.m. får, om det behövs för att utreda brott på vilket fängelse kan följa, fingeravtryck tas också av den som misstänks för brottet utan att vara anhållen eller häktad för detta samt av den som inte är misstänkt för brottet.

Fingeravtryck som tagits med stöd av dessa bestämmelser ska skyndsamt sändas till Rikspolisstyrelsen (7 § förordningen). Nationella fingeravtrycksavdelningen vid Rikskriminalpolisen ansvarar för registrering och kvalitetssäkring av fingeravtryck.

Vad som sagts angående fingeravtryck gäller även handavtryck.

5.3.2 Analys och identifiering

Det huvudsakliga arbetet med analyser av fingeravtryck bedrivs vid SKL och Nationella fingeravtrycksavdelningen vid Rikskriminalpolisen. Dessa framkallar och säkrar spår i form av fingeravtryck på olika typer av undersökningsmaterial. Fingeravtryck måste ges egenskaper som ger en kontrast mot bakgrunden. Därför penslas fingeravtrycket med t.ex. kolpulver eller framkallas genom infärgning. Även andra metoder, t.ex. att få fram en reaktionsprodukt, används. Ett framkallat fingeravtryck säkras genom fotografering.

För att identifiera fingeravtrycket, eller handavtryck, sker en uppkoppling mot en databas benämnd Automatiskt fingerav-

trycksidentifikationssystem (Automated Fingerprint Identification System, AFIS). AFIS är ett bildhanteringssystem som används för att lagra, söka och spåra finger- och handflateavtryck. Systemet gör en digital "karta" över varje fingeravtryck genom att skapa unika matematiska algoritmer baserade på förhållandet mellan olika karakteristika i avtrycket. Sökningar i databasen efter matchande fingeravtryck underlättar analysen av de avtryck som slutligen verifieras manuellt.

5.3.3 Registrering

Den rättsliga regleringen

I 29–31 §§ polisdatalagen finns bestämmelser om bl.a. fingeravtrycksregister. Rikspolisstyrelsen får behandla uppgifter i fingeravtrycksregister för att underlätta identifiering av personer i samband med brott. Uppgifterna får också användas för identifiering av okända personer i andra fall. De får vidare behandlas i förundersökningar och särskilda undersökningar (29 §). Fingeravtrycksregister får endast innehålla uppgifter om den som är misstänkt eller dömd för brott eller som har fått lämna fingeravtryck med stöd av en viss bestämmelse i lagen om särskild utlänningskontroll. Sådana register får inte innehålla uppgifter om fingeravtryck från den som är under femton år. Endast uppgifter om fingeravtryck, signalement, identifieringsuppgifter och ärendenummer får antecknas (30 §).

Bestämmelserna i 29–31 §§ polisdatalagen har emellertid i praktiken inte börjat tillämpas. Enligt punkten 2 i övergångsbestämmelserna till polisdatalagen gäller datalagen (1973:289) för de personregister som den 24 oktober 1998 fördes med Datainspektionens tillstånd. Övergångsbestämmelserna har förlängts flera gånger och senast till den 31 december 2009 (prop. 2008/09:15). Datalagen är således tillämplig, tillsammans med Datainspektionens tillstånd, på fingeravtrycksregistret fram till utgången av detta år, medan bestämmelserna i 29–31 §§ polisda-

talagen inte ska tillämpas. Regleringen av fingeravtrycksregistret överensstämmer dock i stort med polisdatalagens bestämmelser om ändamål och innehåll samt gallring.

Sökningen

I realiteten görs fyra olika typer av sökningar i fingeravtrycksregistret. En sökning kan utgå från ett fingeravtryck som polisen har tagit för att se om personen finns i registret. En annan sökmetod är att utgå från personens fingeravtryck för att knyta vederbörande till okända fingeravtryck som har säkrats på en brottsplats. Vidare kan ett okänt fingeravtryck från en brottsplats användas för en sökning i registret efter en viss person. Ett okänt fingeravtryck kan också kopplas mot andra befintliga okända fingeravtryck.

Det finns vissa möjligheter för svensk polis att söka efter fingeravtryck i en annan medlemsstats register över fingeravtryck. I dessa fall skickar polismyndigheten en kopia av en blankett med personens fingeravtryck, en s.k. 10-fingersblankett, till Rikskriminalpolisens Internationella polisenhet (IPO). IPO scannar in fingeravtrycken från blanketten och sänder dem per e-post till motsvarande myndighet i den andra staten. Om en sökning i det utländska registret ger träff skickas relevanta uppgifter via e-post tillbaka till IPO, som vidarebefordrar uppgifterna till den berörda polismyndigheten.

Gallring

För fingeravtrycksregistret gäller särskilda gallringsbestämmelser som meddelats av Datainspektionen.[34] Bestämmelserna överensstämmer i sak med 31 § polisdatalagen. En misstänkt person ska gallras ur registret när förundersökning eller åtal mot personen

[34] Datainspektionens beslut den 1 december 2005, dnr 698-2005, meddelat med stöd av 6 och 18 §§ datalagen.

läggs ned eller åtal mot personen ogillas. Uppgifterna får dock bevaras längre om andra uppgifter om den registrerade ska behandlas med stöd av polisdatalagens regler om behandling av uppgifter om kvarstående misstankar. Om den registrerade döms, ska uppgifterna gallras senast när uppgifterna gallras ur belastningsregistret.

Under år 2008 gjorde Rikskriminalpolisen en omfattande gallring i sitt fingeravtrycksregister sedan Datainspektionen kritiserat den bristande gallringen av uppgifter.[35] Närmare 100 000 personer, hälften av alla registrerade, gallrades bort enligt uppgift från polisen. Registret gallras nu en gång per månad.

5.4 Fordonsregister

5.4.1 Vägtrafikregistret

I lagen (2001:558) och förordningen (2001:650) om vägtrafikregister finns bl.a. bestämmelser om behandling av personuppgifter i samband med registrering av fordon. Regleringen ligger till grund för det vägtrafikregister som sedan den 1 januari 2009 förs av Transportstyrelsen (tidigare Vägverket). Lagen innehåller bestämmelser om registrering av uppgifter om personer samt om motordrivna fordon och släpfordon i ett särskilt register.

Enligt 12 § lagen om vägtrafikregister ska som huvudregel ett motorfordon vara registrerat för att få användas. Uppgift om vem som äger fordonet är ett krav för att fordonet ska kunna registreras (6 §). I 8 § lagen om vägtrafikregister anges att direktåtkomst till personuppgifter får medges endast för sådana ändamål som anges i 5 § 1–3 samma lag och i enlighet med föreskrifter meddelade av regeringen. Närmare villkor för direktåtkomst till vägtrafikregistret finns i 4 kap. 3–5 §§ förordningen om vägtrafikregister, som bl.a. reglerar behörighets- och säkerhetsfrågor samt sökbegrepp. Direktåtkomst till uppgifter i vägtrafikre-

[35] Datainspektionens beslut den 1 december 2005, Dnr 698-2005, och den 19 november 2007, Dnr 1093-2007.

gistret får endast medges om den utgör en tillåten behandling av personuppgifter enligt personuppgiftslagen (4 kap. 4 § första stycket förordningen).

Eftersom vägtrafikregisterförfattningarna utgör speciallagstiftning har de bestämmelser som reglerar bevarande och gallring av uppgifter, och som i dag finns intagna i förordningen om vägtrafikregister, företräde framför personuppgiftslagen. Beträffande rättelse och skadestånd gäller dock reglerna i personuppgiftslagen (11 § lagen om vägtrafikregister).

5.4.2 EUCARIS

Mellan vägtrafikregistermyndigheterna i vissa av Europeiska unionens medlemsstater, däribland Sverige, förekommer ett automatiskt informationsutbyte genom den tekniska plattformen EUCARIS (European Car and Driving License Information System). EUCARIS är ett samarbete baserat på ett avtal som ingicks av femton av medlemsstaterna i juni 2000.

EUCARIS är ett kommunikationsnätverk och således inget självständigt register. Genom säker inloggning kan vägtrafikregistermyndigheterna i de stater som omfattas av samarbetet göra förfrågningar via nätverket. Svarsformulären är standardiserade.

Uppgifter som omfattas av informationsutbytet är tillverkare och bilmodell, typ av fordon, färg, vilken typ av bränsle fordonet använder och en statussignal som bl.a. indikerar om bilen är stulen eller skrotad. Vissa stater, dock inte Sverige, utbyter även körkortsuppgifter.

När Prümrådsbeslutet ska börja tillämpas kommer enbart en anpassning av vilka uppgifter som lämnas i svarsformuläret att behövas.

6 Rättsliga utgångspunkter

6.1 Inledning

I detta avsnitt redovisas översiktligt vissa internationella överenskommelser och bestämmelser i svensk rätt som antingen allmänt eller i enskildheter har relevans för hur svensk rätt förhåller sig till regleringen i rådsbeslutet (se analys i avsnitt 7).

Avsnittet inleds med en genomgång av internationella åtaganden (avsnitten 6.2.1–6.2.5). Därefter behandlas nationell lagstiftning med fokus på personuppgifter för brottsbekämpning och sekretess (avsnitten 6.3.1–6.3.8). Sist i avsnittet redovisas några aktuella översyner och lagstiftningsärenden, bl.a. förslaget till ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet (avsnitt 6.4).

6.2 Internationella åtaganden

6.2.1 Europakonventionen

Sedan år 1995 gäller den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) som svensk lag.

Enligt artikel 6.1 i Europakonventionen har en person, vid prövningen av hans eller hennes civila rättigheter och skyldigheter eller vid en anklagelse för brott, rätt till domstolsprövning inom skälig tid.

I två avseenden är konventionen av särskild betydelse för personuppgiftsbehandling. Det gäller dels rätten till skydd för bl.a. privat- och familjeliv (artikel 8), dels möjligheten för var och en vars i konventionen angivna fri- och rättigheter har kränkts att få tillgång till ett effektivt rättsmedel inför en nationell myndighet (artikel 13). Bestämmelserna gäller även om det är en offentlig myndighet som inskränkt åtnjutandet av rättigheten eller kränkt någons fri- och rättigheter. En inskränkning är dock tillåten om den sker med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

6.2.2 Dataskyddskonventionen

Europarådets konvention från år 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen) brukar ses som en precisering av artikel 8 i Europakonventionen (se föregående avsnitt). Konventionen trädde i kraft den 1 oktober 1985 och har ratificerats av samtliga medlemsstater i Europeiska unionen.

Konventionen syftar till att säkerställa den enskildes rätt till personlig integritet och att förbättra förutsättningarna för ett fritt informationsflöde över gränserna. Konventionsstaterna är skyldiga att uppfylla vissa principer för dataskydd i sin nationella lagstiftning. Detta innebär att medlemsstaterna ska ha en nationell reglering som föreskriver att personuppgifter som är föremål för automatisk databehandling ska hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål, att uppgifterna måste vara relevanta och förenliga med ändamålen och att uppgifterna ska vara riktiga och aktuella samt inte får bevaras längre än vad som är nödvändigt för ändamålen. Känsliga personuppgifter, t.ex. uppgifter om enskildas ras, politiska tillhörighet eller

religiösa tro samt uppgifter om brott, får behandlas endast om nationell lagstiftning ger ett tillfredsställande skydd.

Konventionen föreskriver att lämpliga skyddsåtgärder ska vidtas för att hindra avsiktlig eller otillåten förstörelse m.m. Vidare finns bestämmelser om registrerade personers möjligheter till insyn i register och rätt att få uppgifter rättade.

Ett tilläggsprotokoll till dataskyddskonventionen antogs av Europarådets ministerkommitté år 2001. Detta innehåller bestämmelser om dataskyddsmyndigheter och överföring av personuppgifter mellan länder. Sverige har ratificerat tilläggsprotokollet.

6.2.3 Europarådets rekommendation No. R (87) 15

Europarådet har tagit fram en särskild rekommendation som reglerar användningen av personuppgifter inom polissektorn. Rekommendationen (No. R [87] 15) innehåller skyddsregler för sådana personuppgifter som polisen samlar in, lagrar, använder eller överför med hjälp av automatiserad behandling i syfte att förhindra och bekämpa brott eller upprätthålla allmän ordning. Endast sådana uppgifter som är nödvändiga för att förhindra en verklig fara eller bekämpa ett visst brott får samlas in, om inte den nationella lagstiftningen tillåter ett mer omfattande uppgiftssamlande. Olika kategorier av lagrade uppgifter ska så långt som möjligt kunna skiljas från varandra efter graden av riktighet och tillförlitlighet. I synnerhet ska uppgifter som grundar sig på fakta kunna skiljas från uppgifter som grundar sig på omdömen eller personliga värderingar.

6.2.4 Dataskyddsdirektivet

Dataskyddsdirektivet[36] syftar till att skapa en gemensam hög nivå på integritetsskyddet och att därigenom möjliggöra ett fritt flöde av personuppgifter mellan medlemsstaterna.

Direktivet innehåller ett flertal materiella bestämmelser som reglerar all hantering av personuppgifter, bl.a. generella regler om vilka krav som ställs vid behandling av personuppgifter.

Direktivet är inte tillämpligt på sådan behandling av personuppgifter som faller utanför gemenskapsrätten, vilket bl.a. innebär att straffrätt och polisverksamhet inte omfattas av tillämpningsområdet.

Dataskyddsdirektivet genomfördes i svensk rätt genom införandet av personuppgiftslagen (se avsnitt 6.3.1).

En närmare beskrivning av direktivet finns i bl.a. Ds 2008:30 s. 34 f.

6.2.5 Europiska unionens stadga om de grundläggande rättigheterna

Europeiska unionens stadga om de grundläggande rättigheterna från år 2000 är en politisk viljeförklaring som syftar till att kodifiera de grundläggande fri- och rättigheter som unionen erkänner. Även om stadgan inte är rättsligt bindande för medlemsstaterna nationellt så binder den unionens egna organ och institutioner samt medlemsstaterna när de tillämpar unionsrätten.

Enligt stadgan har var och en rätt till skydd av de personuppgifter som rör honom eller henne (artikel 8). Uppgifterna ska behandlas lagenligt, för bestämda ändamål och med den berörda personens samtycke eller någon annan legitim eller lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter

[36] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EGT L 281, 23.11.1995, s. 31.

som rör honom eller henne och att få uppgifterna rättade. En oberoende myndighet ska kontrollera att reglerna efterlevs.

6.3 Svensk lagstiftning

6.3.1 Personuppgiftslagen

Lagens tillämpningsområde

Som nämnts ovan har dataskyddsdirektivet införlivats med svensk lagstiftning genom personuppgiftslagen (1998:204). Lagen ersatte den tidigare datalagen (1973:289) och är generellt tillämplig. Den upphävda datalagen gäller dock fortfarande för vissa register på polisområdet, bl.a. fingeravtrycksregistret (se avsnitt 5.3.3).

Personuppgiftslagen ger ett grundläggande integritetsskydd och reglerar hanteringen av personuppgifter. Lagen är subsidiär i förhållande till annan författningsreglering (2 §).

Lagen gäller för all sådan behandling som är helt eller delvis automatiserad (5 §). Den gäller också för annan behandling av personuppgifter om uppgifterna ingår, eller är avsedda att ingå, i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen kompletteras av personuppgiftsförordningen (1998:1191).

Samtidigt som personuppgiftslagen infördes tillskapades särskilda lagar och förordningar, s.k. registerförfattningar, som reglerar behandlingen av personuppgifter inom ett visst verksamhetsområde, för en viss typ av register eller för ett bestämt register. Det finns särreglering för behandling av personuppgifter i brottsbekämpningen, som till stora delar ersätter personuppgiftslagen. Utgångspunkten har varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska

regleras i lag, även om det inte är nödvändigt med lagform enligt grundlagarna.[37]

Grundläggande krav på behandlingen

Bestämning av ändamålen med behandling av personuppgifter är av central betydelse för enskildas integritet. Med behandling avses i sammanhanget varje typ av åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatiserad väg eller inte. Som exempel kan nämnas insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring (3 § personuppgiftslagen).

I 9 § personuppgiftslagen anges grundläggande krav på behandling av personuppgifter som en personuppgiftsansvarig alltid måste följa. Den personuppgiftsansvarige, som oftast är den organisation där personuppgifterna behandlas, ska bl.a. se till att personuppgifterna bara behandlas om det är lagligt och att de alltid behandlas på ett korrekt sätt och i enlighet med god sed (9 § första stycket a och b). Därutöver ska de uppgifter som behandlas vara riktiga och, om det är nödvändigt, aktuella (9 § första stycket g). Alla rimliga åtgärder ska vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen (9 § första stycket h). Personuppgifter får endast bevaras så länge det är nödvändigt med hänsyn till ändamålen med behandlingen (9 § första stycket i). De får vidare endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. De insamlade personuppgifterna får inte senare behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (9 § första stycket c och d). Sistnämnda krav ger uttryck

[37] Prop. 1990/91:60 s. 58 och bet. KU 1990/91:11 s. 11.

för den s.k. finalitetsprincipen. Det finns dock inget som hindrar att insamling sker för flera ändamål samtidigt. Eftersom finalitetsprincipen kan tolkas så att den medger behandling av alla sådana uppgifter som inte är oförenliga med det ändamål för vilka de samlades in kan det finnas skäl att i en registerförfattning ange om de angivna ändamålen är uttömmande.[38]

Förhållandet till offentlighetsprincipen

Bestämmelserna i personuppgiftslagen ska inte tillämpas om de inskränker en myndighets skyldigheter enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter med stöd av offentlighetsprincipen (8 § första stycket). Bestämmelserna i personuppgiftslagen hindrar vidare inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet (8 § andra stycket). Det förutsätts inte att bevarandet är föreskrivet i författning, utan det är tillräckligt att det är fråga om allmänna handlingar.[39]

Tillåten och otillåten behandling

Lagen reglerar uttömmande under vilka förutsättningar behandling av personuppgifter är tillåten (10–12 §§). Vidare föreskrivs att behandling av känsliga personuppgifter som huvudregel är förbjuden (13 §). Känsliga personuppgifter definieras i lagen som uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Från förbudet att behandla känsliga uppgifter görs bl.a. undantag för viss nödvändig behandling för att den registrerades eller annans vitala intressen ska kunna skyddas (se vidare 14–19 §§). Det finns också ett bemyndigande för regeringen, eller den myndighet

[38] Se Sören Öman i Festskrift till Peter Seipel, s. 704 f.
[39] Prop. 1997/98:44 s. 119 f.

regeringen bestämmer, att meddela föreskrifter om ytterligare undantag från förbudet, om det behövs med hänsyn till ett viktigt allmänt intresse (20 §). Sådana föreskrifter finns i 8 § personuppgiftsförordningen.

Som huvudregel är det förbjudet för andra än myndigheter att behandla sådana personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden (21 §). Uppgifter om personnummer och samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl (22 §).

Information och rättelse

Flera bestämmelser i personuppgiftslagen syftar till att trygga den enskildes rätt till information och olika kontrollmöjligheter.

Om uppgifterna samlats in från någon annan än den enskilde, ska den registrerade som huvudregel informeras när uppgifterna registreras, eller, om avsikten med behandlingen är att lämna ut dem till tredje man, när uppgifterna lämnas ut första gången (24 §). Sådan information behöver dock inte lämnas om det finns bestämmelser om registreringen eller utlämnande av uppgifterna i lag eller författning eller om det skulle vara omöjligt eller kräva en oproportionerligt stor arbetsinsats att informera. I en särskild bestämmelse preciseras vad informationen ska omfatta (25 §). Den personuppgiftsansvarige är skyldig att efter ansökan, en gång per år, gratis informera om huruvida och i så fall vilka uppgifter om sökanden som behandlas, ändamålet med behandlingen, varifrån uppgifterna kommer och till vem de lämnas ut (26 §). Från uppgiftsskyldigheten undantas dock bl.a. sådana uppgifter som omfattas av sekretess eller tystnadsplikt gentemot den registrerade (27 §).

Utöver den personuppgiftsansvariges allmänna skyldighet enligt 9 § att se till att de personuppgifter som behandlas är ade-

kvata och relevanta i förhållande till ändamålen med behandlingen kan den registrerade begära att den personuppgiftsansvarige snarast ska *rätta*, *blockera* eller *utplåna* sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller i enlighet med föreskrifter som har meddelats med stöd av lagen (28 §). Om felaktiga personuppgifter har lämnats ut till tredje man, ska denne i vissa fall informeras om korrigeringen.

Säkerhet vid behandlingen

I 30–32 §§ finns allmänna bestämmelser om säkerheten vid behandling av personuppgifter. Bestämmelserna avser att trygga både den tekniska säkerheten och att de personer som behandlar uppgifterna har tillräckliga instruktioner för att behandla uppgifterna på ett korrekt sätt. Den personuppgiftsansvarige har ett stort ansvar för säkerheten. Tillsynsmyndigheten kan bl.a. i enskilda fall besluta om vilka säkerhetsåtgärder som den personuppgiftsansvarige ska vidta.

Överföring av personuppgifter till tredje land

Det är som huvudregel förbjudet att till tredje land föra över personuppgifter under behandling, eller för behandling, om landet inte har en adekvat skyddsnivå för personuppgifter (33 §). Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständligheter som har samband med överföringen. Ett antal omständigheter som anses speciellt viktiga räknas upp särskilt.

Av 34 § följer bl.a. att det är tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter. Ytterligare undantag från kravet på viss skyddsnivå kan beslutas efter bemyndigande (35 §). I bilagor till personuppgiftsförordningen anges vissa län-

der som enligt särskilt beslut av Europeiska gemenskapernas kommission anses ha en adekvat skyddsnivå för behandlingen av personuppgifter eller som har slutit avtal med Europeiska unionen om överföring av vissa slags uppgifter.

Tillsyn

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen (2 § personuppgiftsförordningen). Inspektionen är även tillsynsmyndighet enligt de särskilda registerförfattningarna.

För sin tillsyn har Datainspektionen rätt att på begäran få tillgång till de personuppgifter som behandlas och upplysningar och dokumentation av behandlingen och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter (43 §). Om tillsynsmyndigheten efter begäran inte kan få tillräckligt underlag för att konstatera att behandlingen är laglig, får myndigheten vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på annat sätt än att lagra dem (44 §). Tillsynsmyndigheten har vidare bl.a. rätt att hos länsrätten ansöka om att sådana personuppgifter som har behandlats på ett felaktigt sätt ska utplånas (47 §).

Sanktioner

En personuppgiftsansvarig är skadeståndsskyldig i de fall behandling av personuppgifter i strid med personuppgiftslagen orsakar den registrerade skada (48 §). Skadeståndsansvaret är i princip strikt. Den registrerade ska visa att det förekommit en felaktig behandling och att denna skadat eller kränkt honom eller henne.

Lagen innehåller också en straffbestämmelse (49 §). Till böter eller fängelse i högst sex månader döms bl.a. den som uppsåtligen eller av grov oaktsamhet behandlar personuppgifter i strid med bestämmelserna om behandling av känsliga personuppgifter

eller för över personuppgifter till tredjeland i strid med bestämmelserna i 33–35 §§.

Lagen beskrivs närmare i bl.a. Ds 2008:30 s. 36 f.

6.3.2 Polisdatalagen

Allmänt

Polisdatalagen innehåller både allmänna regler om behandling av personuppgifter i polisiärt arbete och regler om vissa särskilda register. Den gäller utöver personuppgiftslagen vid behandling av personuppgifter i polisens verksamhet och i polisverksamhet vid Ekobrottsmyndigheten för att

- förebygga brott och andra störningar av den allmänna ordningen och säkerheten,
- övervaka den allmänna ordningen och säkerheten,
- hindra störningar av den allmänna ordningen och säkerheten samt ingripa när något sådant inträffat, eller
- bedriva spaning och utredning i fråga om brott som hör under allmänt åtal (1 §).

Lagen gäller inte för behandling av personuppgifter med stöd av lagen om belastningsregister, lagen om misstankeregister, lagen om Schengens informationssystem eller lagen (2006:444) om passagerarregister (1 § tredje stycket).

I 5 § regleras vilken behandling av känsliga personuppgifter, dvs. uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexuella läggning (13 § personuppgiftslagen) som är tillåten. Vidare finns bestämmelser om utlämnande av uppgifter (6–8 §§). I detta sammanhang är den bestämmelse som reglerar möjligheten att lämna ut uppgifter till utländska myndigheter och mellanfolkliga organisationer av särskilt intresse (7 §). Som huvudregel får uppgifter lämnas ut om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Regeringen får vidare

meddela föreskrifter om att uppgifter på begäran får lämnas till en polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten ska kunna förebygga, upptäcka, utreda eller beivra brott. Sådana föreskrifter finns i 18 § polisdataförordningen. Regleringen är sekretessbrytande.

Därutöver finns bestämmelser om rättelse och skadestånd (9 §) som i princip gäller även för behandling av personuppgifter i register som inte är automatiserade (2 §).

Information till den registrerade, säkerhet vid behandlingen, rättelse och skadestånd

Eftersom polisdatalagen inte innehåller några regler om information till den registrerade, säkerhet vid behandling, rättelse och skadestånd gäller beträffande dessa frågor de allmänna reglerna i personuppgiftslagen. I 9 § polisdatalagen finns en hänvisning till personuppgiftslagens bestämmelser om rättelse och skadestånd.

Register som regleras särskilt i polisdatalagen

Det finns ett antal register som regleras särskilt i lagen. Detta gäller bl.a. kriminalunderrättelseregister (17–21 §§) och Säkerhetspolisens s.k. SÄPO-register (32–35 §§). Även DNA-register (22–28 §§) samt fingeravtrycks- och signalementsregister (29–31 §§) regleras särskilt.

Avsnitt 5 innehåller en redovisning av bl.a. reglerna om DNA-register och fingeravtrycksregister.

6.3.3 Sekretesslagen

I sekretesslagen (1980:100) finns bestämmelser som gör det möjligt för myndigheter att utbyta uppgifter trots att dessa omfattas av sekretess.

En utgångspunkt i sekretesslagen är att en uppgift som omfattas av sekretess inte får röjas för en utländsk myndighet eller mellanfolklig organisation. I två situationer får dock sådana uppgifter röjas (1 kap. 3 § tredje stycket). Den ena är när utlämnandet sker i enlighet med en särskild föreskrift i lag eller annan författning. En uttrycklig bestämmelse om att uppgifter får lämnas till en utländsk myndighet eller mellanfolklig organisation bryter alltså sekretess enligt 1 kap. 3 § tredje stycket. Den andra är när uppgiften i motsvarande fall skulle få lämnas till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas. Sistnämnda regel är avsedd att tillämpas restriktivt.

Sekretessbelagda uppgifter får vidare lämnas ut från en myndighet till en annan om det är nödvändigt för att den *utlämnande* myndigheten ska kunna fullgöra sin verksamhet (1 kap. 5 §). Denna sekretessbrytande bestämmelse är också avsedd att tillämpas restriktivt. Något sekretessgenombrott medges inte på den grunden att den *mottagande* myndigheten behöver uppgifterna i sin verksamhet.

Inom vissa myndighetsområden, bl.a. polisens brottsbekämpande verksamhet, är det i ganska stor utsträckning nödvändigt att lämna ut sekretessbelagda uppgifter för att över huvud taget kunna genomföra exempelvis förhör. I ett internationellt perspektiv är ett typiskt exempel att svenska myndigheter i samband med begäran om rättslig hjälp i en förundersökning lämnar uppgifter som omfattas av sekretess enligt 5 kap. 1 § och 9 kap. 17 § till en utländsk åklagar- eller polismyndighet i syfte att få ett visst förhör genomfört. Om det är nödvändigt för en myndighet att lämna ut sekretessbelagda uppgifter för att denna ska kunna fullgöra sin egen verksamhet står det i regel klart att det är förenligt med svenska intressen att lämna ut uppgifterna.

Med stöd av en sekretessbrytande bestämmelse i 9 kap. 17 § kan uppgifter vidare lämnas ut enligt vad som föreskrivs i bl.a. polisdatalagen och i förordningar som meddelats med stöd av den lagen (9 kap. 17 § sjätte stycket 3). Bestämmelsen infördes i samband med att den absoluta sekretessen för polisregister av-

skaffades.[40] Det bakomliggande syftet var bl.a. att myndigheterna inte skulle behöva förlita sig på en sekretessprövning i de fall där det i författning anges att uppgifter får lämnas ut. I 6–8 §§ polisdatalagen finns bestämmelser om att uppgifter får lämnas ut. Sådana bestämmelser finns även i polisdataförordningen (se bl.a. 8, 10, 17, 17 a och 18 §§).

Ytterligare sekretessbrytande bestämmelser finns i 14 kap. sekretesslagen. Om en uppgiftsskyldighet följer av lag eller förordning hindrar sekretess inte att uppgifter lämnas ut till en annan myndighet (14 kap. 1 §). Vidare kan uppgifter, med vissa undantag, lämnas ut när de behövs i bl.a. förundersökningar (14 kap. 2 §).

Av den s.k. generalklausulen i 14 kap. 3 § första stycket följer vidare att sekretessbelagda uppgifter som huvudregel får lämnas ut till en annan myndighet efter en intresseavvägning som innebär att det ska vara uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda.

Bedömningen av om en uppgift kan lämnas ut görs av den myndighet som innehar uppgiften, utom i de fall där utlämnandebestämmelsen har konstruerats så att uppgiften alltid ska lämnas ut om det begärs.

Generellt gäller vidare att en myndighet på begäran av en annan ska lämna ut uppgifter i den mån hinder inte möter på grund av sekretess eller arbetets behöriga gång (15 kap. 5 §). Det innebär att sådana uppgifter som en myndighet begär att få del av från en annan myndighet ska lämnas ut om någon av de ovan nämnda sekretessbrytande bestämmelserna är tillämpliga eller om de begärda uppgifterna är offentliga.

[40] Prop. 1997/98:97.

6.3.4 Lagen om internationellt polisiärt samarbete

Lagen (2000:343) om internationellt polisiärt samarbete reglerar samarbetet mellan svenska brottsbekämpande myndigheter och motsvarande myndigheter i andra medlemsstater i Europeiska unionen samt Norge och Island. Schengensamarbetet, men även visst övrigt polissamarbete som är konventionsbundet, regleras i lagen. Lagen omfattar inte bara polismän utan även tulltjänstemän och kustbevakningstjänstemän, när de enligt lag eller annan författning har polisiära befogenheter.

I lagen finns bl.a. en bestämmelse som reglerar hur uppgifter som har mottagits från andra stater får användas (3 §), vad som brukar kallas användningsbegränsning. Om en svensk myndighet har fått upplysningar eller bevismaterial från en annan stat för att användas i underrättelseverksamhet om brott eller vid utredning av brott, och gäller på grund av överenskommelse med den andra staten villkor som begränsar möjligheten att utnyttja materialet, ska svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning. Detta gäller även för överenskommelser med mellanfolkliga organisationer.

Det informationsutbyte som sker inom ramen för Schengensamarbetet regleras i huvudsak i lagen om Schengens informationssystem (se avsnitt 6.3.8).

6.3.5 Lagen om vissa former av internationellt samarbete i brottsutredningar

Lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar genomför bl.a. rådets rambeslut 2002/465/RIF av den 13 juni 2002 om gemensamma utredningsgrupper (1 §).

Syftet med rambeslutet är att förbättra det polisiära och straffrättsliga samarbetet mellan Europeiska unionens medlemsstater i kampen mot den gränsöverskridande brottsligheten. Genom en överenskommelse får behöriga myndigheter i två eller flera medlemsstater inrätta en gemensam utredningsgrupp för

brottsutredningar. Lagen tillämpas när det finns en sådan överenskommelse mellan en eller flera myndigheter i Sverige och motsvarande myndigheter i en eller flera andra medlemsstater. De utredningsgrupper som inrättas med stöd av någon annan internationell överenskommelse omfattas inte av lagen.[41]

I lagen finns bl.a. särskilda bestämmelser om användningsbegränsningar för uppgifter som mottas eller lämnas. Har en svensk myndighet fått uppgifter genom en gemensam utredningsgrupp som inrättats med stöd av lagen och gäller på grund av en överenskommelse villkor som begränsar möjligheten att använda uppgifterna, ska en svensk myndighet följa villkoren oavsett vad som annars är föreskrivet i lag eller författning (5 §). Om uppgifter eller bevismaterial överlämnas från en svensk myndighet till en sådan utredningsgrupp får överlämnandet förenas med de villkor som är nödvändiga av hänsyn till enskilds rätt eller från allmän synpunkt (6 §). Villkor som strider mot en överenskommelse enligt 1 § får dock inte ställas upp. Den svenska myndighet som har överlämnat material med villkor får på begäran av en myndighet i en annan stat medge undantag från villkoren (7 §). Detsamma gäller för villkor som följer direkt av en överenskommelse som träffats med stöd av 1 §.

6.3.6 Lagen om internationellt tullsamarbete

Tullverkets samarbete med tullmyndigheter och andra behöriga myndigheter i andra stater regleras i lagen (2000:1219) om internationellt tullsamarbete. I syfte att förhindra, upptäcka, utreda och beivra överträdelser av tullbestämmelser ska Tullverket eller annan behörig svensk myndighet bistå utländsk myndighet och mellanfolklig organisation. Förutom Tullverket är Rikspolisstyrelsen, polismyndigheter, Kustbevakningen och Statens jordbruksverk behöriga myndigheter (1 kap. 5 §). Tullverket har an-

[41] Detta gäller t.ex. gemensamma utredningsgrupper som upprättats med stöd av artikel K 3 i fördraget om Europeiska unionen om ömsesidigt bistånd och samarbetet mellan tullförvaltningar (tullsamarbetskonventionen).

svaret för samordningen av samarbetet. De svenska myndigheterna kan agera endast inom ramen för sina befogenheter enligt nationell rätt (1 kap. 3 §).

Tullsamarbetet består bl.a. i att staterna självmant eller efter ansökan delger varandra uppgifter som behövs för samarbetet. Svensk myndighet har också rätt att inleda utredning om överträdelse av tullbestämmelser i en annan stat. I en sådan utredning får en utländsk tjänsteman närvara. Åtgärder får inte vidtas med stöd av samarbetet om dessa strider mot svensk författning eller svenska allmänna rättsprinciper.

Lagen innehåller särskilda användningsbegränsande bestämmelser som dels ålägger svenska myndigheter att följa de villkor om användning av lämnade uppgifter som andra länder kan ställa upp, dels ger svenska myndigheter möjlighet att på motsvarande sätt ställa upp villkor för användandet av uppgifter som lämnas ut (2 kap. 7 § och 4 kap. 2 §). Regleringen ska tillämpas restriktivt och villkoren ska vara nödvändiga.[42]

6.3.7 Lagen om internationell rättslig hjälp i brottmål

I lagen (2000:562) om internationell rättslig hjälp i brottmål föreskrivs skyldighet att på en utländsk myndighets begäran genomföra bl.a. förhör under förundersökning, bevisupptagning, telefonförhör, husrannsakan och vissa andra tvångsmedel (1 kap. 2 §). Vidare regleras hur Sverige kan begära rättslig hjälp utomlands (3 kap.).

I förordningen (2000:704) om internationell rättslig hjälp i brottmål finns verkställighetsbestämmelser.

Lagen är med något undantag generell och gäller i förhållande till alla stater, även om dessa inte har tillträtt samma konventioner om rättslig hjälp i brottmål som Sverige.

En utländsk stats begäran om rättslig hjälp i Sverige handläggs av åklagare och domstol, under förutsättning att åtgärden kan

[42] Prop. 1999/2000:122 s. 43.

vidtas enligt svensk lag under en förundersökning eller rättegång. I vissa fall får rättslig hjälp beviljas även om den misstänkta gärningen inte utgör brott enligt svensk lagstiftning (2 kap. 2 §).

I 2 kap. finns allmänna bestämmelser om förfarandet vid en ansökan om rättslig hjälp i Sverige. I princip används samma förfarande som vid motsvarande svensk åtgärd under förundersökning eller rättegång (2 kap. 10 §).

I lagen finns särskilda användningsbegränsande bestämmelser. Dessa gäller såväl om en svensk myndighet i ett ärende om rättslig hjälp mottar uppgifter eller bevisning från en annan stat med villkor som begränsar möjligheterna att använda uppgifterna eller bevisningen (5 kap. 1 §) som i de fall där en svensk myndighet lämnar rättslig hjälp och då ställer upp villkor som är påkallade med hänsyn till enskilds rätt eller som är nödvändiga ur allmän synpunkt (5 kap. 2 §).

6.3.8 Lagen om Schengens informationssystem

I en särskild databas, Schengens informationssystem (SIS), som beskrivits i avsnitt 4.2.6, kan varje medlemsstat föra in uppgifter om personer eller föremål som är efterlysta eller på annat sätt eftersöks, tillsammans med en begäran om att en viss åtgärd ska vidtas om personen eller föremålet påträffas. I lagen (2000:344) om Schengens informationssystem regleras behandlingen av personuppgifter i den nationella delen av SIS. Lagen gäller utöver personuppgiftslagen och innehåller bl.a. regler om vilka uppgifter som får registreras och i vilka syften detta får ske (3 och 4 §§), en särskild bestämmelse om att känsliga uppgifter inte får registreras (7 §) samt bestämmelser om gallring, rättelse och skadestånd (11–13 §§).

Lagen innehåller också en regel om användningsbegränsning (10 §). En svensk myndighet får inte utnyttja en uppgift i registret för något annat syfte än det som den registrerande staten har angett vid registreringen. Om den registrerande staten har

lämnat sitt samtycke, får dock en svensk myndighet använda uppgiften för ett annat ändamål.

6.4 Aktuella översyner och lagstiftningsärenden

6.4.1 Ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet

Ett förslag till en ny reglering, som ska ersätta polisdatalagen och polisdataförordningen, har presenterats i departementspromemorian Behandling av personuppgifter i polisens brottsbekämpande verksamhet (se Ds 2007:43). Promemorian har remissbehandlats och en proposition planeras.

Den föreslagna lagen är heltäckande och reglerar, med något undantag, all polisens behandling av personuppgifter i den brottsbekämpande verksamheten vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten, dvs. hos de myndigheter som bedriver polisverksamhet. Lagen är däremot inte tillämplig i fråga om annan verksamhet som polisen bedriver, t.ex. hjälpande verksamhet eller verksamhet för upprätthållande av ordning och säkerhet utan anknytning till brottsbekämpning. För behandling av personuppgifter i sådan verksamhet gäller personuppgiftslagen. Precis som nu faller lagen om belastningsregister, lagen om misstankeregister, lagen om Schengens informationssystem och lagen om passagerarregister utanför lagens tillämpningsområde.

Den föreslagna regleringen bygger på en uppdelning mellan å ena sidan ”behandling av gemensamt tillgängliga uppgifter” och å andra sidan annan behandling. Begreppet ”gemensamt tillgängliga” har införts som ett nytt teknikneutralt begrepp i stället för begreppen register och databas som tidigare använts för att definiera uppgifter som har gjorts tillgängliga för en större krets. Uppgifter som endast ett fåtal bestämda personer har rätt att ta del av anses inte vara gemensamt tillgängliga, medan däremot uppgifter som en annan brottsbekämpande myndighet har till-

gång till genom direktåtkomst alltid är gemensamt tillgängliga. I fråga om uppgifter om resultat av DNA-analyser föreslås att uppgifterna inte får göras gemensamt tillgängliga (se 3 kap. 2 § andra stycket). Uppgifterna får däremot, om förutsättningarna i övrigt är uppfyllda, behandlas i särskilda register enligt 4 kap. i den föreslagna lagen. Vidare får ett utlåtande över den eventuella identifiering som har gjorts och vad som förekommit vid analysarbetet göras gemensamt tillgängligt.

I lagförslaget regleras ett antal register särskilt (4 kap.), bl.a. de DNA-register som finns i dag och fingeravtrycksregister. För behandling av uppgifter om resultat av DNA-analyser föreslås en reglering som gör tydlig skillnad mellan å ena sidan behandling av DNA-profiler och å andra sidan den eventuella identifiering som DNA-analysen leder fram till. Utöver behandling i DNA-register föreslås behandling av DNA-profiler få förekomma endast inom ramen för förundersökning. För de särskilda DNA-registren, där DNA-profiler och DNA-spår registreras, föreslås inga stora förändringar. Samma myndigheter som i dag har direktåtkomst till de register som innehåller resultat av DNA-analyser (DNA-register, utredningsregister och spårregister) föreslås få det även i framtiden (jfr 11 § polisdataförordningen). Vidare ska polismyndigheter och åklagarmyndigheter även fortsättningsvis ha begränsad åtkomst till uppgifter om en person förekommer i registret eller inte. När det gäller uppgifter i fingeravtrycks- och signalementsregister föreslås samtliga brottsbekämpande myndigheter, med undantag för åklagare, medges direktåtkomst till personuppgifter. I den nya lagen ges också utrymme för regeringen att meddela föreskrifter om direktåtkomst till vissa uppgifter i polisens register i de fall där det finns folkrättsligt bindande åtaganden som riksdagen godkänt att medge sådan åtkomst. Vidare föreslås regler om sekretessgenombrott för uppgifter i bl.a. DNA-register och fingeravtrycksregister. Utan hinder av sekretess enligt 9 kap. 17 § sekretesslagen ska uppgifter ur fingeravtrycksregister kunna lämnas till Rikspolisstyrelsen, polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen eller Skatteverket, om

myndigheten behöver uppgiften i sin brottsbekämpande verksamhet. Vidare ska uppgift om huruvida någon förekommer i register med uppgifter om DNA-analyser under samma förutsättningar lämnas ut till polis- och åklagarmyndigheter. I den mån andra sekretessbestämmelser aktualiseras måste emellertid enligt förslaget, precis som i dag, göras en bedömning i det enskilda fallet av om sekretessen hindrar att uppgifterna lämnas till en annan brottsbekämpande myndighet.

6.4.2 Ny offentlighets- och sekretesslag

Regeringen överlämnade i oktober 2008 en remiss till Lagrådet om en ny offentlighets- och sekretesslag. Lagrådet yttrade sig den 21 januari 2009. Utgångspunkten för lagrådsremissen är vissa förslag av Offentlighets- och sekretesskommittén (SOU 2003:99). Lagrådsremissen innehåller bl.a. en redaktionell omarbetning av sekretesslagen, förändringar av sekretessbestämmelsernas skaderekvisit och förslag till en teknikneutral bestämmelse om sekretessmarkering. Den nya lagen föreslås träda i kraft den 30 juni 2009.

Beträffande den sekretessreglering som behandlats i avsnitten ovan innebär regeringens förslag inga sakliga förändringar. Bestämmelserna har dock omarbetats. Detta gäller bl.a. 9 kap. 17 § sekretesslagen som föreslås ersättas av dels en bestämmelse om sekretess i förundersökning m.m. (17 kap. 1 § i lagförslaget), dels en bestämmelse om sekretess i underrättelseverksamhet m.m. (17 kap. 2 § i lagförslaget).

6.4.3 Vägtrafikregisterutredningen

Regeringen beslutade den 15 maj 2008 att tillkalla en särskild utredare med uppgift att se över lagen (2001:558) om vägtrafikregister med tillhörande förordning och föreslå mer ändamålsenliga regler (dir. 2008:53 och tilläggsdir. 2009:2). Huvudsyftet är

att förenkla, modernisera och effektivisera regelverket. Utredaren ska särskilt beakta de behov som finns hos registerhållande myndighet (i dag Transportstyrelsen) av att behandla uppgifter och personuppgifter i ett trafikregister eller en trafikdatabas och de behov som finns hos andra myndigheter eller berörda aktörer av att på olika sätt ta del av eller behandla sådana uppgifter och personuppgifter.

Uppdraget ska redovisas den 4 januari 2010.

7 Genomförandet av rådsbeslutet

7.1 Allmänna utgångspunkter

7.1.1 Vad innebär rådsbeslutet?

Den internationella polissamarbetet har successivt utökats och har numera många olika former, särskilt inom Europeiska unionen. Den möjlighet som rådsbeslutet ger medlemsstaterna att automatiskt ta del av vissa uppgifter i varandras register bör ses i ljuset av detta. Rådsbeslutets syfte är att man ska utnyttja den kunskap som finns genom att förverkliga tillgänglighetsprincipen. Principen innebär i korthet att en tjänsteman vid en brottsbekämpande myndighet i en medlemsstat som behöver viss information för att utföra sina uppgifter ska kunna få den från en annan medlemsstat som har informationen i fråga.

Det särskilda informationsutbyte som regleras i rådsbeslutet innebär ett enklare och snabbare sätt att få viktig information som kan vara avgörande för att klara upp brott eller för att avföra misstänkta som är oskyldiga. Genom rådsbeslutet utvecklas och förändras framför allt formerna för utbyte av DNA-profiler och fingeravtrycksuppgifter mellan medlemsstaterna. De sökningar rådsbeslutet medger omfattar till största delen sådana registeruppgifter som redan i dag utbyts mellan medlemsstaterna. Den stora skillnaden i förhållande till dagens ordning är att utbytet av uppgifter i ökad utsträckning kan ske på elektronisk väg och att den som behöver informationen omedelbart får besked om det finns någon uppgift av intresse eller inte. Även ett negativt besked kan ha stor betydelse i en brottsutredning.

De uppgifter som kan anses vara mest integritetskänsliga, DNA-profiler och fingeravtrycksuppgifter, får dock bara kontrolleras och jämföras utan att några identitetsuppgifter röjs. I de fortsatta kontakterna mellan staterna ska reglerna om internationell rättslig hjälp tillämpas. Det nya informationsutbytet ger således stora fördelar samtidigt som den enskildes integritet värnas.

Genomförandet av rådsbeslutet kräver svenska lagstiftningsåtgärder. I propositionen om godkännande av Prümrådsbeslutet övervägde regeringen på ett allmänt plan vilka lagändringar som aktualiseras (prop. 2007/08:83). I detta avsnitt redovisas de författningsändringar som bedöms vara nödvändiga och lämpliga för att genomföra de obligatoriska delarna av rådsbeslutet i svensk rätt. Utöver förslag till lagändringar presenteras också förslag till vissa förordningsändringar, i syfte att ge en mer heltäckande bild av den framtida regleringen.

7.1.2 Dispositionen av avsnittet

Inledningsvis redovisas rådsbeslutets allmänna bestämmelser (avsnitten 7.2–7.4). Sedan behandlas frågor med anknytning till DNA-register och utbyte av DNA-profiler (avsnitten 7.5–7.8), utbyte av fingeravtrycksuppgifter (avsnitt 7.9) samt fordonsuppgifter (avsnitt 7.10). I avsnitt 7.11 avhandlas svenska myndigheters möjlighet att få tillgång till uppgifter i andra medlemsstaters register. Därefter tas vissa gemensamma frågor upp. Avsnitt 7.12 behandlar sekretess. Förslag till svenskt kontaktställe för förmedling av uppgifter redovisas i avsnitt 7.13. I avsnitt 7.14 redovisas informationsutbytet inför vissa större evenemang. Avsnitt 7.15 behandlar skyldigheten att bistå en annan medlemsstat med praktisk hjälp eller expertis och avsnitt 7.16 andra former av gränsöverskridande samarbete. I de följande avsnitten behandlas frågor rörande skyddet av den enskildes integritet (7.17), korrigering och bevarande av personuppgifter (7.18), kontroll och tillsyn över behandlingen (7.19) samt rätten för enskilda att

överklaga och begära skadestånd vid felaktig personuppgiftsbehandling (7.20). Sist behandlas rådsbeslutets effekter på andra myndigheter än polisen (avsnitt 7.21 och 7.22) samt kraven på teknisk anpassning (7.23).

7.2 Rådsbeslutets syfte och tillämpningsområde

Bedömning: Rådsbeslutets allmänna bestämmelser om syfte och tillämpningsområde innehåller inga förpliktelser för medlemsstaterna. Några lagstiftningsåtgärder krävs därför inte.

Skälen för bedömningen: Rådsbeslutets första kapitel innehåller allmänna bestämmelser som inte ålägger medlemsstaterna några särskilda skyldigheter. Bestämmelserna avgränsar emellertid rådsbeslutets tillämpningsområde. Av artikel 1 följer att informationsutbytet i första hand omfattar myndigheter som ansvarar för att förebygga och utreda brott. Vidare avgränsas tillämpningsområdet till bestämmelser om villkoren och förfarandet för:

- automatisk överföring av DNA-profiler, fingeravtrycksuppgifter och vissa uppgifter ur nationella fordonsregister,
- översändande av uppgifter i samband med större evenemang med gränsöverskridande verkningar,
- översändande av uppgifter för att förebygga terroristbrott, och
- ett fördjupat gränsöverskridande polissamarbete.

Rådsbeslutet omfattar i viss del enbart polisiärt samarbete (artikel 17), men är i huvudsak generellt och omfattar allt rättsligt samarbete inom beslutets tillämpningsområde (jfr preambeln).

Med hänsyn till rådsbeslutets syfte och tillämpningsområde kan det antas att genomförandet i första hand påverkar polisens internationella samarbete och i mindre utsträckning motsvarande

verksamhet vid Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket (se vidare avsnitt 7.21). Rådsbeslutet kommer framför allt att påverka det arbete med DNA-analyser och jämförelse av fingeravtryck som sker vid SKL respektive på Nationella fingeravtrycksavdelningen vid Rikskriminalpolisen och som har beskrivits närmare i avsnitt 5.

Eftersom bestämmelserna angående syfte och tillämpningsområde inte innehåller några bindande förpliktelser kräver de inga lagstiftningsåtgärder.

7.3 Författningsregleringen

Bedömning: Den lagstiftning som rådsbeslutet kräver ska i huvudsak genomföras i polisdatalagen, lagen om internationellt polisiärt samarbete och lagen om vägtrafikregister. Dessutom krävs viss reglering i förordning.

Skälen för bedömningen: I propositionen om godkännande av Prümrådsbeslutet redovisade regeringen en preliminär bedömning av i vilken utsträckning nuvarande lagstiftning måste ändras (prop. 2007/08:83). Eftersom propositionen inte innehöll några lagförslag diskuterades inte närmare var de nya bestämmelserna skulle placeras.

Det är uppenbart att det krävs vissa författningsändringar för att genomföra rådsbeslutet, framför allt vad gäller utbyte av information i DNA-, fingeravtrycks- och vägtrafikregister. Den nya regleringen kan knytas till flera olika författningar.

Polisdatalagen (1998:622) reglerar behandling av personuppgifter i polisens verksamhet, däribland ändamålen med DNA- och fingeravtrycksregister och villkoren för behandling av uppgifter i sådana register. Lagen (2001:558) om vägtrafikregister med tillhörande förordning reglerar behandling av personuppgifter i vägtrafikregistret. Polisdatalagen är sedan flera år föremål för en genomgripande översyn (se Ds 2007:43 och avsnitt 6.4.1)

och även vägtrafikregisterregleringen ses över (se avsnitt 6.4.3). Gällande rätt måste trots detta anpassas till kraven i rådsbeslutet, eftersom detta ska vara genomfört innan översynerna har resulterat i ny lagstiftning. Vissa ändringar krävs alltså i dessa författningar.

Givetvis måste den behandling av personuppgifter som följer av rådsbeslutet fogas in i den nationella lagstiftning som redan gäller för sådan behandling, dvs. personuppgiftslagen (1998:204) och särbestämmelser i förhållande till den lagen. Personuppgiftslagen är generellt tillämplig på behandling av personuppgifter, om det inte finns avvikande bestämmelser i särskild författning (2 § personuppgiftslagen). Både polisdatalagen och lagstiftningen om trafikregister innehåller bestämmelser som avviker från personuppgiftslagen och gäller utöver denna. Genomförandet av rådsbeslutet kräver speciella detaljbestämmelser om behandling av personuppgifter som avviker från de generella reglerna i polisdatalagen. De nya reglerna låter sig också svårligen inordnas i den lagen. Det är därför bättre att samla reglerna om Prümrådssamarbetet i någon av de lagar som behandlar internationellt samarbete. Om bestämmelser om behandling av personuppgifter i polisens verksamhet ska gälla *utöver* polisdatalagen måste detta framgå. Med tanke på det pågående lagstiftningsarbetet har valts en lösning som i minsta möjliga utsträckning påverkar den generella författningsregleringen i polisdatalagen och som innebär att detaljerna regleras i andra författningar. Därmed måste det i polisdatalagen klargöras att det finns särskilda bestämmelser i annan lag som gäller utöver bl.a. lagens gallringsregler. En sådan lagstiftningsteknik är naturligtvis inte optimal, men den enda möjliga i sammanhanget, eftersom rådsbeslutets specifika reglering måste genomföras i svensk rätt.

Vad som nu har sagts om svårigheten att förena de nya bestämmelserna om personuppgiftsbehandling med regleringen i polisdatalagen gäller också för regleringen beträffande vägtrafikregister. Även där pågår utredningsarbete som siktar till att ersätta den nuvarande lagstiftningen, varför samma lösning bör väljas i det fallet.

Rådsbeslutet skapar också möjligheter för svenska myndigheter att söka i andra medlemsstaters register samt reglerar visst polisiärt samarbete över gränserna i övrigt. Bestämmelser om internationellt polisiärt samarbete finns i olika lagar. Delar av det polisiära samarbetet, främst Schengensamarbetet och det polisiära samarbetet i Öresundsregionen, regleras i lagen (2000:343) om internationellt polisiärt samarbete. I lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar regleras bl.a. formerna för inrättande av och deltagande i utredningsgrupper mellan myndigheter i en eller flera medlemsstater i Europeiska unionen. Reglerna om rättsligt bistånd finns huvudsakligen i lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) med tillhörande förordning.

Utöver vissa nödvändiga ändringar i polisdatalagen och lagen om vägtrafikregister finns det inte någon på förhand given plats för nya bestämmelser om utländska myndigheters tillgång till uppgifter i svenska register och svenska myndigheters tillgång till utländska myndigheters registeruppgifter. Varken lagen om internationellt polisiärt samarbete, lagen om vissa former av internationellt samarbete i brottsutredningar eller någon annan författning framstår som en självklar plats att införliva rådsbeslutets förpliktelser i. Det skulle i och för sig vara möjligt att placera bestämmelserna i en helt ny lag. Det som talar för en sådan lösning är att den svenska lagstiftning som genomför rådsbeslutet då skulle finnas samlad, vilket normalt ger överskådlighet. För att en ny lag ska bli fullständig torde emellertid krävas att fler bestämmelser än annars ges lagform. Vidare skulle det leda till en dubbelreglering i vissa frågor i förhållande till de lagar som reglerar respektive register. Reglerna om polisiärt och rättsligt samarbete är redan spridda i ett flertal författningar. Det är därför trots allt tveksamt om en helt ny författning skulle leda till bättre överskådlighet. Något som också talar mot en ny författning är att rådsbeslutets reglering visserligen spänner över ett brett fält, men har beröringspunkter framför allt med samarbetet enligt Schengenkonventionen. Vid en samlad bedömning väger

skälen för att genomföra rådsbeslutet i någon av de befintliga lagarna tyngst.

Övervägande skäl talar för att den anpassning av lagstiftningen som rådsbeslutet kräver i huvudsak bör genomföras i lagen om internationellt polisiärt samarbete. Sistnämnda lag tillämpas på polisiärt samarbete mellan brottsbekämpande myndigheter i Sverige och i andra stater anslutna till Schengenkonventionen, dvs. andra medlemsstater i Europeiska unionen samt Norge och Island. Lagen är inte begränsad till samarbete i brottsutredningar, vilket är fallet med lagen om vissa former av internationellt samarbete i brottsutredningar. Eftersom rådsbeslutet har ett vidare tillämpningsområde än sistnämnda lag, nämligen ordningshållning och förebyggande terrorismbekämpning, ligger det närmare till hands att i huvudsak införa den nya regleringen i lagen om internationellt polisiärt samarbete. Viss reglering i LIRB aktualiseras också. Utöver lagändringar krävs kompletterande reglering i förordning.

På sikt förefaller en samlad översyn av de olika författningarna om internationellt polisiärt samarbete och utbyte av information, i syfte att åstadkomma en mera enhetlig och lättillämpad reglering, inte bara önskvärd utan nödvändig. Brottslighetens ökade internationalisering och den snabba utvecklingen av det polisiära samarbetet mellan medlemsstaterna i Europeiska unionen talar för detta. Ju fler nya samarbetsformer som överenskoms, desto angelägnare blir det att se över regelverket.

7.4 Definitioner

Bedömning: De begrepp som definieras i rådsbeslutet kräver inga lagstiftningsåtgärder.

Skälen för bedömningen: I rådsbeslutet definieras begreppen behandling av personuppgifter, automatisk sökning, förseende

med en beteckning och spärrande (se artikel 24.1). I genomförandebeslutet finns vissa ytterligare definitioner (artikel 2).

Definitionen av *behandling av personuppgifter* (artikel 24.1 a) har en direkt motsvarighet i svensk rätt. Med det begreppet avses i rådsbeslutet all behandling av personuppgifter eller en räcka av behandlingar med eller utan hjälp av automatiska förfaranden, t.ex. insamling, registrering, lagring, bearbetning och spridning. I 3 § personuppgiftslagen finns en i sak motsvarande definition. Övriga definitioner har inte någon direkt motsvarighet i svensk rätt.

Enligt rådsbeslutet avses med *automatisk sökning* ett förfarande varigenom det nationella kontaktstället ges direkt tillgång till ett annat organs automatiska databas så att en förfrågan besvaras fullständigt automatiskt (artikel 24.1 b). Definitionen utesluter behandling i manuella register. I den svenska lagstiftningen motsvaras den närmast av begreppet direktåtkomst. I dag används begreppet direktåtkomst i olika registerförfattningar, men med något varierande innebörd. Det som enligt vedertagen uppfattning karaktäriserar direktåtkomst är främst att den som är ansvarig för informationen inte har kontroll över vilka uppgifter som en mottagare vid ett visst tillfälle tar del av, s.k. automatiserad tillgång, och att mottagaren av informationen inte kan påverka innehållet i det informationssystem eller register som hanterar informationen (se t.ex. prop. 2004/05:164 s. 83 och 2007/08:126 s. 74).

Innebörden av *förseende med en beteckning* är att registrerade personuppgifter märks, dock inte i syfte att begränsa den framtida behandlingen av dem (artikel 24.1 c). Begreppet *spärrande* innebär däremot att registrerade personuppgifter märks i syfte att begränsa den framtida behandlingen av uppgifterna (artikel 24.1 d). I 3 § personuppgiftslagen definieras begreppet ”blockering”, som innebär ”en åtgärd som vidtas för att personuppgifterna ska vara förknippade med information om att de är spärrade och om anledningen till spärren och för att personuppgifterna inte ska lämnas ut till tredje man annat än med stöd av 2 kap. tryckfrihetsförordningen.” Som regeringen tidigare har

konstaterat är blockering ett något snävare begrepp än rådsbeslutets definition av spärrande (se prop. 2007/08:83 s. 39). Det väsentliga är dock att svensk lagstiftning i sak kan garantera att uppgifter ”spärras” på det sätt och i de situationer som rådsbeslutet förutsätter.

Det kan konstateras att vilka begrepp som används är en nationell angelägenhet, så länge rådsbeslutets förpliktelser uppfylls och uppgiftsutbytet mellan medlemsstaterna inte försvåras. Något sakligt skäl att införa nya begrepp med anledning av Prümrådsbeslutet finns inte, men däremot måste de förfaranden som avses ha motsvarigheter i svensk rätt. Begreppen som definieras i rådsbeslutet kräver därför inga lagstiftningsåtgärder i sig. Det finns dock anledning att återkomma till vissa begrepp i avsnitt 7.18.

7.5 DNA-register

Bedömning: Befintliga svenska DNA-register, dvs. DNA-registret, utredningsregistret och spårregistret, uppfyller rådsbeslutets krav på att medlemsstaterna ska ha nationella register med DNA-analyser för brottsutredningar.

Förslag: Sverige ska underrätta rådets generalsekretariat om att DNA-registret, utredningsregistret och spårregistret omfattas av rådsbeslutet.

Skälen för förslaget och bedömningen: Rådsbeslutet föreskriver att medlemsstaterna ska ha egna nationella databaser med DNA-analyser för brottsutredningar (artikel 2.1). Utbytet av uppgifter med stöd av rådsbeslutet är decentraliserat och bygger – till skillnad från bl.a. Eurodac[43]– på en kommunikationsmodell som benämns ”alla–till–alla” (”any–to–any”). Det

[43] Rådets förordning (EG) nr 2725/2000 av den 11 december 2000 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av Dublinkonventionen. Se avsnitt 4.4.

innebär att det inte finns någon central databas eller server. Uppgifterna hämtas i stället direkt från medlemsstaternas nationella databaser.

Begreppet databas definieras inte i rådsbeslutet, men tar sikte på strukturerade uppgifter av visst slag som finns samlade och som har gjorts tillgängliga för en större krets. I sak motsvarar det begreppet register.

Regleringen i polisdatalagen utgår från att uppgifter om resultatet av DNA-analyser ska behandlas i särskilda register (se avsnitt 5.2.2). Det finns ett DNA-register med uppgifter om dömda (23 och 24 §§ polisdatalagen), ett utredningsregister med uppgifter om skäligen misstänkta personer (24 a §) och ett spårregister med uppgifter om DNA-spår från oidentifierade personer (25 och 26 §§). Spårregistret innehåller framför allt oidentifierade DNA-profiler från spår på eller i nära anslutning till brottsplatser. Det förhållandet att spårregistret enbart innehåller DNA-profiler från oidentifierade personer innebär att kravet i artikel 2.2 på att oidentifierade DNA-profiler ska kunna särskiljas är uppfyllt.

I förslaget till ny reglering av behandlingen av personuppgifter i polisens brottsbekämpande verksamhet föreslås att de nu aktuella registren ska regleras på i huvudsak samma sätt som i dag (se Ds 2007:43 s. 279 f. och 460 f.).

I Sverige finns redan de DNA-register som behövs för att uppfylla kraven i rådsbeslutet. Några nya databaser behöver därför inte inrättas. I sammanhanget kan det finnas skäl att se till att DNA-registren konsekvent benämns DNA-registret, utredningsregistret och spårregistret. Inget hindrar att ett sådant register innehåller olika delar, med delvis samma innehåll, om detta bedöms vara en lämplig och ändamålsenlig lösning för att möjliggöra direktåtkomst för kontaktställen i andra stater.

Förutsättningarna för att behandla uppgifter i registren regleras enligt rådsbeslutet i nationell rätt (artikel 2.1). Det innebär att det även i fortsättningen är svensk rätt som reglerar bl.a. vilka personuppgifter som får registreras och de närmare förutsättningarna för detta.

Enligt rådsbeslutet ska medlemsstaterna underrätta rådets generalsekretariat om de nationella register över DNA-analyser som omfattas av detta (artikel 2.3). Underrättelsen bör för svensk del omfatta DNA-registret, utredningsregistret och spårregistret.

7.6 Begreppet DNA-profil

Förslag: I definitionen av begreppet DNA-analys görs ett tillägg som klargör att lagen endast omfattar analys av prov från människor. Vidare införs en definition av begreppet DNA-profil. Av denna ska framgå dels att det är fråga om resultatet av en DNA-analys, dels att resultatet presenteras som en kombination av siffror eller bokstäver.

Skälen för förslaget: Begreppet DNA-profil används genomgående i rådsbeslutet, men definieras inte. I polisdatalagen används begreppet ”DNA-analys” för att beteckna det förfarande som leder fram till en DNA-profil och det som registreras benämns ”resultatet av DNA-analyser”. Att föra in nya begrepp i registerförfattningar eller att ändra i befintliga sådana bör normalt undvikas. I vissa fall är det emellertid nödvändigt att se över begreppsbilden.

De uppgifter som efter en DNA-analys får registreras anges i 24, 24 a och 25 §§ polisdatalagen. Vid polisdatalagens tillkomst framhölls vikten av att begränsa rätten att spara resultat av DNA-analyser till sådana mer allmänna upplysningar som inte kan ge upplysning om den registrerades personliga egenskaper. Det som får registreras begränsas därför till uppgifter som ger information om den registrerades identitet, samt uppgifter om i vilket ärende analysen har gjorts och vem analysen avser (prop. 1997/98:97 s. 143 f.). Några ändringar i detta avseende gjordes inte i samband med att användningen av DNA-teknik inom brottsbekämpningen utvidgades (prop. 2005/06:29). I dag regi-

streras uppgifter om det aktuella ärendet och vem analysen avser samt brottskod och misstankenummer. Brottskoden används för statistiska ändamål och misstankenumret för att säkerställa spårbarheten i de fall där personuppgifterna är osäkra eller misstänks vara falska. DNA-profilerna i registren presenteras som en kombination av siffror eller bokstäver.

En DNA-profil består, enligt artikel 2 c i genomförandebeslutet, av en bokstavs- eller nummerkod som representerar en rad identifikationsuppgifter i den icke-kodifierade delen av mänskligt DNA. Definitionen motsvarar de DNA-profiler som registreras i de svenska DNA-registren.

Det finns goda skäl för att låta begreppet ”DNA-profil” ersätta beteckningen ”uppgifter om resultat av DNA-analyser” i polisdatalagen. Ett skäl är att begreppet används i rådsbeslutet. Ett annat är att det är missvisande att, som i dag, i polisdatalagen ange innehållet i registren som ”uppgifter om resultatet av DNA-analyser” när det som registreras enbart är DNA-profilen samt uppgifter om den undersöktes identitet, om den är känd, (se prop. 2005/06:29 s. 22) och vissa administrativa uppgifter.

Termen DNA-profil bör således införas. Då är det också nödvändigt att definiera vad som avses med DNA-profil. Av definitionen ska framgå dels att det är fråga om resultatet av en DNA-analys, dels att resultatet presenteras som en kombination av siffror eller bokstäver. För att tydliggöra att polisdatalagen enbart reglerar DNA-analys av prov från människor bör vidare ett tillägg göras i definitionen av begreppet DNA-analys så att det framgår att begreppet endast omfattar analys av prov från en människa.

7.7 Utbyte av DNA-profiler

7.7.1 Automatisk sökning och jämförelse i svenska register

Förslag: I polisdatalagen införs en bestämmelse som öppnar möjlighet att behandla vissa uppgifter i DNA-register om det krävs för att uppfylla en internationell överenskommelse som riksdagen har godkänt. I lagen om internationellt polisiärt samarbete och i förordning regleras under vilka förutsättningar ett utländskt kontaktställe får söka i svenska DNA-register samt hur automatisk sökning i registren och automatisk jämförelse av DNA-profiler ska gå till.

Skälen för förslagen

Innehållet i rådsbeslutet

Medlemsstaterna ska enligt rådsbeslutet ges direkt tillträde till referensuppgifter i varandras DNA-register. De ska också ha rätt att behandla uppgifter i form av DNA-profiler genom *automatiska sökningar* i dessa (artikel 3.1 och 24). Sökningarna får göras i enskilda fall och i överensstämmelse med den nationella lagstiftningen i den ansökande medlemsstaten. Sökningarna ska göras av ett nationellt kontaktställe. Om en träff uppkommer, dvs. om det konstateras att två DNA-profiler överensstämmer, ska den ansökande medlemsstaten automatiskt få del av referensuppgifter bestående av DNA-profilen från den icke-kodifierade delen av DNA:t med en tillhörande sifferuppgift (artikel 2.2). Referensuppgifterna röjer alltså inte identiteten på den person som DNA-profilen härrör från. I de fall där det inte konstateras någon överensstämmelse ska den ansökande medlemsstaten automatiskt underrättas om detta. Om den DNA-profil som sökningen avser härrör från en oidentifierad person, och någon överensstämmelse inte konstateras, får DNA-profilen översändas till övriga medlemsstaters databaser.

Utöver för registrering i dataskyddssyfte, får referensuppgifterna enbart behandlas för att fastställa om jämförda DNA-profiler överensstämmer och för att utarbeta eller lämna in en begäran om rättslig hjälp med kompletterande uppgifter. Genom den valda lösningen uppstår inga risker från integritetssynpunkt, eftersom identiteten på den person som DNA-profilen tillhör inte avslöjas. Man kan uttrycka det så att det alltid är fråga om jämförelse mellan anonyma DNA-profiler.

Efter en gemensam överenskommelse mellan berörda stater får DNA-profiler också *jämföras automatiskt*, om den ansökande medlemsstatens nationella lagstiftning tillåter det. Detta sökförfarande innebär att en medlemsstats samtliga oidentifierade DNA-profiler jämförs med referensuppgifter i andra medlemsstaters nationella DNA-register (artikel 4.1). Om en översänd DNA-profil motsvarar en profil som ingår i en annan stats databaser, ska de referensuppgifter som överensstämmer utan dröjsmål tillställas den sökande medlemsstatens kontaktställe (artikel 4.2). Inte heller i dessa fall avslöjas identiteten på den som DNA-profilen tillhör.

Enligt rådsbeslutet är det en förutsättning, oavsett sökförfarande, att sökningen görs ”i samband med brottsutredningar”.

Nya regler om sökning i DNA-registren

Rådsbeslutet förbättrar medlemsstaternas möjligheter att snabbt och enkelt utbyta DNA-profiler i samband med brottsutredningar. Som regeringen redovisar i propositionen om godkännande av Prümrådsbeslutet visade det sig omgående att tillämpningen av Prümfördraget ledde till att ett antal DNA-profiler som fanns registrerade i en medlemsstat kom till användning i en annan medlemsstats brottsbekämpning (prop. 2007/08:83 s. 61).

Genomförandet av rådsbeslutet förutsätter att svensk rätt medger uppgiftsbehandling i de svenska DNA-registren i enlighet med rådsbeslutets två sökförfaranden. Båda dessa saknar motsvarighet i dagens lagstiftning. Det kan i och för sig hävdas

att uppgiftsbehandling med anledning av en utländsk brottsutredning omfattas av ändamålsbestämmelsen i 22 § polisdatalagen (se regeringens analys i prop. 2007/08:83 s. 12). I förtydligande syfte bör dock paragrafen ändras så att det klart framgår att behandling som består i att kontaktstället i en annan stat söker i svenska DNA-register har rättsligt stöd.

För att andra stater, under de förutsättningar som i övrigt gäller enligt svensk rätt, ska kunna söka i de svenska DNA-registren och automatiskt få uppgift om en översänd DNA-profil stämmer överens med någon DNA-profil i registren (*automatisk sökning*) krävs att staterna ges direktåtkomst till uppgifter i registren. Dagens lagstiftning medger inte detta, varför rådsbeslutet kräver nya regler som möjliggör sådan direktåtkomst.

Den generella rätten att kunna behandla uppgifter i DNA-registret, utredningsregistret och spårregistret bör regleras i polisdatalagen, medan bestämmelser om åtkomst och sökförfarande bör placeras i lagen om internationellt polisiärt samarbete och i förordning. I polisdatalagen bör man införa en regel som tillåter sådan behandling som krävs för att uppfylla förpliktelserna i en internationell överenskommelse som riksdagen har godkänt. För närvarande pågår förhandlingar med Norge och Island om att dessa länder ska få delta i Prümsamarbetet (se avsnitt 8). På sikt kan det inte uteslutas att även andra stater kommer att ansöka om deltagande i samarbetet. Den nya regleringen bör därför inte begränsas enbart till utbyte av DNA-profiler med andra medlemsstater i Europeiska unionen, utan utformas generellt så att den omfattar varje stat med vilken det finns en bindande överenskommelse om samarbete av detta slag. Med en regel som kräver att riksdagen har godkänt överenskommelsen, får man en flexibel reglering utan att ge avkall på rättssäkerheten.

Regleringen måste vidare utformas så att den säkerställer att kontaktstället i den andra staten inte kan identifiera den person som DNA-profilen tillhör. Enligt rådsbeslutet ska nämligen andra medlemsstaters direkta tillgång till uppgifter i DNA-register begränsas till uppgifter som inte röjer identiteten på den person som DNA-profilen härrör från. Detta är en fråga som får

lösas tekniskt, genom begränsad åtkomst till uppgifterna i DNA-registren (se även avsnitt 7.23). Lagstiftningen bör utformas så att det tydligt framgår att rätten till direktåtkomst endast omfattar sådana registeruppgifter som inte röjer identiteten på den person som uppgifterna avser (referensuppgifter). Sökningen ska resultera i ett automatiskt meddelande om den sökta DNA-profilen finns i registren eller inte. Även detta är i första hand en teknisk fråga.

En särskild fråga är hur man ska hantera den situationen att det finns behov av att på förfrågan från den mottagande staten skicka viss kompletterande information. Som exempel kan nämnas kurvor som åskådliggör analysresultaten (s.k. elektroferogram) eller andra uppgifter som verifierar analysresultaten, men som inte röjer identiteten på den person uppgifterna hänför sig till. Sådana uppgifter torde kunna överlämnas inom ramen för Prümrådssamarbetet, så länge det är fråga om uppgifter som har karaktären av referensuppgifter, dvs. uppgifter som inte gör att den som DNA-profilen härrör från kan identifieras. När det gäller identitetsuppgifter och annan information rörande den person som DNA-profilen tillhör aktualiseras i stället rättslig hjälp i annan form (se avsnitt 7.7.2).

Automatiska jämförelser förutsätter att svensk rätt medger att andra medlemsstaters oidentifierade DNA-profiler (s.k. öppna spår), efter överenskommelse mellan staterna (”by mutual consent” enligt den engelska texten), får behandlas i de svenska DNA-registren och jämföras automatiskt med referensuppgifterna i dessa. Oidentifierade DNA-profiler hanteras för svensk del i spårregistret (se avsnitt 5.2.2). Automatiska jämförelser måste emellertid omfatta sökningar i samtliga svenska DNA-register för att kraven i rådsbeslutet ska uppfyllas. I 26 § polisdatalagen regleras uttömmande hur uppgifter i det svenska spårregistret får behandlas. Uppgifterna i registret får jämföras med analysresultat i de svenska registren som inte kan hänföras till en identifierbar person (dvs. med andra analysresultat i spårregistret), med uppgifter som finns i DNA-registret och med uppgifter som kan hänföras till en person som är skäligen misstänkt

för brott (dvs. uppgifter i undersökningsregistret). Eftersom rådsbeslutet förutsätter att uppgifter i andra medlemsstaters register kan jämföras generellt med uppgifter i bl.a. spårregistret måste paragrafen som reglerar det registret ändras. Det bör införas en bestämmelse som gör det möjligt att jämföra utländska spår med uppgifter i spårregistret. Någon förändring av möjligheterna för svenska myndigheter att söka i registret är däremot inte aktuell. Eftersom det inte finns några motsvarande begränsningar för sökning i de andra två registren behöver de bestämmelserna inte ändras.

Förutsättningarna för automatiska jämförelser mellan DNA-profiler bör också regleras i lagen om internationellt polisiärt samarbete och i förordning. De nya reglerna bör ange under vilka förutsättningar kontaktställen i andra stater får göra automatisk jämförelse av sina staters oidentifierade DNA-profiler med svenska DNA-profiler. Regleringen bör även här göras generell, dvs. inte begränsas till enbart samarbete mellan medlemsstater i Europeiska unionen, eftersom man som tidigare nämnts kan förutse att även andra stater i framtiden kan komma att associeras till rådsbeslutet genom särskilt avtal.

Även om andra stater ges rätt till direktåtkomst till vissa uppgifter i DNA-register ska sökningarna kanaliseras via det nationella kontaktstället. Den valda lösningen underlättar möjligheterna att i efterhand kontrollera att uppgiftsbehandlingen har varit korrekt. I avsnitt 7.13 diskuteras vilken myndighet som ska vara svenskt kontaktställe.

Svenska myndigheters möjligheter att göra sökningar i andra staters register behandlas i avsnitt 7.11.

7.7.2 Den fortsatta handläggningen

Om det vid en automatisk sökning eller en automatisk jämförelse konstateras att översända DNA-profiler överensstämmer med DNA-profiler i svenska register regleras frågan om vilka personuppgifter och vilken ytterligare information som får över-

sändas uteslutande av den tillfrågade medlemsstatens lagstiftning, inkluderande reglerna om internationell rättslig hjälp (artikel 5). Det innebär att samma regler som gäller för informationsutbyte i allmänhet tillämpas vid bedömningen av i vilken omfattning namn och andra personuppgifter som är direkt kopplade till DNA-profilen ska översändas till en annan medlemsstat, t.ex. födelsetid och adress. I prop. 2007/08:83 s. 15–17 finns en utförlig beskrivning av vilka uppgifter som kan bli aktuella. Utöver namn, personnummer och adressuppgifter, som är direkt kopplade till DNA-profilen, kan det bl.a. bli aktuellt att lämna uppgifter ur belastningsregistret och misstankeregistret; se 11 och 12 §§ lagen (1998:620) om belastningsregister samt 9 och 10 §§ lagen (1998:621) om misstankeregister. Eftersom all handläggning i detta skede faller utanför rådsbeslutet aktualiseras inte några lagändringar.

7.8 Rättslig hjälp med provtagning och fastställande av DNA-profil

Förslag: Genom ett tillägg i lagen om internationell rättslig hjälp i brottmål ska åklagare under vissa förutsättningar kunna besluta om rättslig hjälp med att samla in och analysera DNA-prov från en person som vistas här i landet samt till en annan stat översända den DNA-profil som fastställts genom analysen. En särskild regel om förstörande av DNA-proven införs.

Skälen för förslaget

Innehållet i rådsbeslutet

Om det i en annan medlemsstat pågår en brottsutredning eller ett straffrättsligt förfarande angående en person och det saknas

en DNA-profil för vederbörande i den staten, ska enligt rådsbeslutet under vissa förutsättningar rättslig hjälp kunna ges med att samla in och analysera DNA-prov, om personen vistas i en annan medlemsstat (artikel 7). DNA-profilen ska därefter sändas till den begärande staten. Skyldigheten att ge sådan rättslig hjälp förutsätter att den ansökande medlemsstaten meddelar för vilket ändamål DNA-profilen behövs, att det av ansökan framgår att det hade funnits förutsättningar för insamling och undersökning av materialet om personen hade vistats i den ansökande staten samt att nationell rätt i den anmodade staten medger både att DNA-prov samlas in och analyseras för ändamålet och att DNA-profilen översänds.

Nuvarande möjligheter att ge rättslig hjälp

Frågor om internationell rättslig hjälp i brottmål regleras framför allt i lagen om internationell rättslig hjälp i brottmål (LIRB).

En uttalad målsättning med LIRB är att svenska domstolar och åklagare ska kunna lämna rättslig hjälp i brottmål till utländska myndigheter med alla de åtgärder som kan vidtas i en svensk förundersökning eller rättegång (prop. 1999/2000:61 s. 79 f.). Att staterna ska bistå varandra med rättslig hjälp i så stor utsträckning som möjligt är också en utgångspunkt för 1959 års Europarådskonvention om ömsesidig rättslig hjälp i brottmål (artikel 1), som Sverige har tillträtt, och för konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (2000 års konvention).

LIRB omfattar bl.a. hjälp med åtgärder som avses i 28 kap. rättegångsbalken (1 kap. 2 § 5 LIRB). DNA-prov tas genom kroppsbesiktning enligt 28 kap. 12, 12 a eller 12 b § rättegångsbalken (se avsnitt 5.2.1). Förutsättningarna för att lämna rättslig hjälp beror på vad som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång (2 kap. 1 § LIRB). Regleringen i LIRB innebär således att DNA-prov i och för sig kan tas på begäran av en utländsk myndighet.

Enligt huvudregeln om kroppsbesiktning i 28 kap. 12 § rättegångsbalken får prov tas från den som är skäligen misstänkt för ett brott på vilket fängelse kan följa för att utröna omständigheter som är av betydelse för utredningen av brottet. Salivprov för DNA-analys (men inte andra prov) får enligt 28 kap. 12 b § rättegångsbalken tas vid misstanke om brott på vilket fängelse kan följa från personer som över huvud taget inte är misstänkta eller där misstanken inte når upp till nivån skälig misstanke. För sådana prov krävs dels att det finns synnerlig anledning att anta att provet är av betydelse för utredningen av brottet, dels att provet tas i identifieringssyfte. Dessa regler kan tillämpas vid rättslig hjälp.

Även 28 kap. 12 a § rättegångsbalken innehåller en regel om tagande av DNA-prov i form av salivprov. Sådana prov får tas från den som är skäligen misstänkt, men enligt den paragrafen är syftet enbart att registrera personens DNA-profil. Den bestämmelsen kan dock inte tillämpas vid rättslig hjälp, eftersom prov endast får tas i syfte att göra en DNA-analys av provet och registrera uppgifter om resultatet av analysen i det utredningsregister eller det DNA-register som förs med stöd av polisdatalagen (prop. 2005/06:29 s. 38 f.). Den nuvarande lagstiftningen tillåter alltså inte sådan provtagning om syftet är att en utländsk myndighet ska kunna registrera DNA-profilen.

Det finns inte heller någon regel som ger stöd för att svenska myndigheter ska kunna bearbeta provet, dvs. göra en DNA-analys på begäran av en annan stat. Den föreslagna regeln i 22 § polisdatalagen tar enbart sikte på behandlingen av DNA-profiler.

En ny regel om framtagande av DNA-profil

Utbytet av DNA-profiler mellan stater bör ses mot bakgrund av att det kommer att effektivisera brottsbekämpningen. Som tidigare nämnts har det visat sig vara effektivt att kontrollera de DNA-profiler som finns registrerade, men det finns även behov av att kunna få hjälp med att fram nya DNA-profiler från perso-

ner som befinner sig i andra stater. Eftersom rättslig hjälp i form av kroppsbesiktning för tagande av DNA-prov, i likhet med andra straffprocessuella tvångsmedel, regleras i LIRB är det naturligt att annan rättslig hjälp med anknytning till sådana prov också regleras där.

Det bör införas en särskild regel i LIRB om rättslig hjälp med framtagande av DNA-profil. Från integritetssynpunkt är det till fördel om DNA-analysen görs i det land där provet tas och att DNA-profilen sänds över, eftersom den inte är möjlig att tyda utan tillgång till särskild expertis och inte innehåller någon annan genetisk information. Regeln om rättslig hjälp med framtagande av DNA-profil bör därför vara generell, dvs. kunna tillämpas gentemot alla stater. En sådan lösning har också den fördelen att en svensk myndighet som har behov av ett DNA-prov och framställning av DNA-profil från någon som befinner sig i en annan stat alltid kan utlova motsvarande hjälp.

För närvarande finns det inte några enhetliga regler för DNA-analys, men arbete pågår för att i första hand medlemsstater i Europeiska unionen ska närma sig varandra i detta avseende. Eftersom olika stater tillämpar skilda kriterier för DNA-analys kan visserligen hävdas att det praktiska behovet av en generell regel inte är så stort. Trots detta är emellertid en enhetlig reglering av möjligheterna att bistå med rättslig hjälp att föredra.

Kravet på att rättslig hjälp ska kunna lämnas aktualiserar också frågan om dubbel straffbarhet, dvs. om det ska krävas att gärningen ska vara straffbar även i Sverige för att rättslig hjälp ska ges. Dubbel straffbarhet förutsätter inte att den gärning som ansökan avser direkt ska kunna hänföras under en viss svensk straffbestämmelse. Det är tillräckligt att den aktuella gärningstypen är kriminaliserad i Sverige.

Den nuvarande regleringen i LIRB innebär att rättslig hjälp med tvångsmedel enbart ges i de fall där det föreligger dubbel straffbarhet, om det inte finns någon avvikande bestämmelse i lagen. Frågan är om detta ska gälla även för rättslig hjälp med tagande av DNA-prov enligt rådsbeslutet. Såväl integritetsskäl som att detta krav redan gäller för rättslig hjälp i Sverige i form

av kroppsbesiktning (2 kap. 2 § LIRB och prop. 1999/2000:61 s. 108 och 190) talar för att kravet på dubbel straffbarhet bör upprätthållas. Rådsbeslutet hindrar inte detta. För att rättslig hjälp med DNA-prov ska kunna ges med stöd av rådsbeslutet krävs alltså att den gärning som den andra statens begäran baseras på är kriminaliserad i Sverige.

Genom den tidigare föreslagna ändringen i 22 § polisdatalagen blir översändandet av DNA-profilen tillåtet. Däremot får den framtagna profilen inte registreras i något svenskt DNA-register.

En särskild fråga är hanteringen av de DNA-prov som tas för en annan stats räkning. Enligt 27 a § polisdatalagen ska ett DNA-prov förstöras senast sex månader efter det att provet togs. I vissa fall ska provet förstöras tidigare, men de bestämmelserna har knutits till utfallet av sådan utredning och lagföring som sker i Sverige. Ett DNA-prov innehåller mer integritetskänslig information än själva DNA-profilen, eftersom det ur provet är möjligt att analysera fram uppgifter om en person och dennes egenskaper. Av integritetsskäl bör därför DNA-prov inte bevaras längre än nödvändigt (se prop. 2005/06:29 s. 33). Sådana prov som har tagits som ett led i rättslig hjälp bör i princip kunna förstöras så snart analysen av provet har färdigställts. Med tanke på att det för närvarande inte finns någon gemensam standard för DNA-analys och DNA-profiler skulle det dock kunna inträffa att analysen behöver göras om i något avseende för att den ska vara användbar i den andra staten. Sakliga skäl talar därför för att DNA-proven bör bevaras en kortare tid efter analysen. En sådan ordning får anses vara mindre integritetskränkande för den enskilde än att provtagningen i form av kroppsbesiktning kanske måste göras om och värnar dessutom rättssäkerheten genom möjligheten att komplettera och verifiera uppgifter. Den tid som proven sparas bör vara så kort som möjligt. När det gäller DNA-prov som tas i svenska förundersökningar är huvudregeln att proven ska förstöras senast sex månader efter provtagningen, men i vissa fall tidigare med hänsyn till utgången av det ärende i vilket provet har tagits. Om den regeln skulle göras tillämplig på

prov som tas som ett led i Prümsamarbetet skulle alla prov i praktiken kunna sparas i sex månader. Med hänsyn till det begränsade praktiska behovet av att spara proven, att proven av integritetsskäl alltid bör sparas kortast möjliga tid och att det inte finns någon enhetlig bevarandetid, bör det införas en särskild regel om förstörande av DNA-prov som har tagits på begäran av annan stat. En lämplig avvägning kan vara att proven ska förstöras inom två månader efter det att de har tagits.

Svenska myndigheter bör givetvis ha samma möjligheter att begära rättslig hjälp i andra stater med tagande av DNA-prov och genomförande av DNA-analys som dessa har att få rättslig hjälp i Sverige. En särskild regel om detta bör införas i LIRB.

7.9 Fingeravtrycksuppgifter

7.9.1 Sökning i svenska fingeravtrycksregister

Förslag: I polisdatalagen införs en bestämmelse som öppnar möjlighet att behandla uppgifter i fingeravtrycksregister om det krävs för att uppfylla förpliktelserna i en internationell överenskommelse som riksdagen har godkänt. Vidare ändras övergångsbestämmelserna till polisdatalagen så att lagen blir tillämplig även på fingeravtrycksregister. I lagen om internationellt polisiärt samarbete regleras under vilka förutsättningar ett utländskt kontaktställe får söka i svenska fingeravtrycksregister och hur automatiska sökningar ska ske.

Skälen för förslaget: Enligt rådsbeslutet ska medlemsstaterna ges tillgång till referensuppgifter i varandras fingeravtrycksregister (artikel 8 och 9). Med referensuppgifter avses fingeravtrycksuppgifter och en sifferbeteckning, men däremot inte uppgifter som röjer identiteten på den som avtrycken härrör från. Med fingeravtryck jämställs handavtryck (artikel 2 i genomförandebeslutet). Automatiska sökningar ska enligt beslutet få gö-

ras i syfte att förebygga och utreda brott. Vad som avses med automatisk sökning förklaras närmare i artikel 24. Referensuppgifterna får enbart behandlas för att fastställa om jämförda fingeravtrycksuppgifter överensstämmer eller för att utarbeta eller lämna in en begäran om rättslig hjälp i de fall där fingeravtrycken överensstämmer. Dessutom får uppgifterna behandlas för registrering i dataskyddssyfte (artikel 26.2).

I genomförandebeslutet preciseras de tekniska förutsättningarna för utbyte och sökning av fingeravtrycksuppgifter (artikel 12–14). Bestämmelserna reglerar bl.a. kvaliteten på översända fingeravtrycksuppgifter, säkerheten vid översändandet av uppgifter och sökningskapacitet. Den mottagande staten ska utan dröjsmål kontrollera kvaliteten på översända uppgifter genom ett helt automatiskt förfarande. Är uppgifterna inte lämpliga för en automatisk jämförelse, ska den anmodade medlemsstaten omedelbart underrätta den begärande medlemsstaten. Vidare föreskrivs att en begäran ska behandlas inom 24 timmar genom ett helt automatiskt förfarande (artikel 14.2 i genomförandebeslutet).

Som redovisats i avsnitt 5.3.3 är det inte polisdatalagen, utan den numera upphävda datalagen (1973:289) tillsammans med Datainspektionens tillstånd, som reglerar behandlingen av personuppgifter i fingeravtrycksregister (se punkten 2 i övergångsbestämmelserna till polisdatalagen samt prop. 2000/01:91 s. 9). Denna reglering medger inte att utländska myndigheter ges direktåtkomst till fingeravtrycksregister på det sätt som rådsbeslutet föreskriver. Eftersom datalagen är upphävd kan den inte ändras. Det är inte heller möjligt att genom författning ändra i villkoren för Datainspektionens tillstånd. Genomförandet av rådsbeslutet kräver därför andra åtgärder.

I avvaktan på en ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet torde den enda möjliga lagstiftningsmetoden för att anpassa regleringen rörande fingeravtrycksregister till rådsbeslutets bestämmelser vara att ändra övergångsbestämmelserna till polisdatalagen och göra lagen tillämplig på de fingeravtrycksregister som nu förs med

Datainspektionens tillstånd. Endast då kan den övriga reglering som behövs för genomförandet möjliggöras. I praktiken torde skillnaden inte bli så stor, eftersom Datainspektionens tillstånd motsvarar regleringen i polisdatalagen om fingeravtrycksregister. Bestämmelserna i polisdatalagen ger emellertid inte stöd för den speciella form av direktåtkomst som rådsbeslutet föreskriver. Därför krävs en ny bestämmelse i polisdatalagen som möjliggör sådan behandling i fingeravtrycksregister som krävs för att uppfylla förpliktelserna i en internationell överenskommelse, i detta fall Prümrådsbeslutet. Rådsbeslutet förutsätter att behandlingen kan ske både för brottsutredning och för att förebygga brott. Någon utvidgning av ändamålen med fingeravtrycksregistret bör inte göras, eftersom rådsbeslutet inte syftar till att ändra den nationella behandlingen och den nyss nämnda regeln täcker de sökningar som görs av utländska kontaktställen.

Konsekvenserna av förslaget är att den behandling som i dag sker med stöd av Datainspektionens tillstånd måste anpassas till bestämmelserna i den nuvarande polisdatalagen (jfr prop. 2007/08:6 och 2008/09:15). Ur rättssäkerhetssynpunkt är det en fördel om behandlingen i fingeravtrycksregister, som omfattar ett stort antal personer, sker med stöd av en modernare lagstiftning än datalagen och Datainspektionens tillstånd. Vad som kan tala mot lösningen att genom ändringar i övergångsbestämmelserna nu göra polisdatalagen tillämplig är dock att det kan anses olämpligt att i avvaktan på det pågående lagstiftningsarbetet ändra i befintlig reglering (se bl.a. regeringens bedömning i prop. 2005/06:29 s. 32). För att uppfylla skyldigheterna i rådsbeslutet inom föreskriven tid är det emellertid nödvändigt med omedelbara författningsändringar. Det är således inte möjligt att avvakta att en ny lagstiftning för polisens behandling av personuppgifter beslutas, särskilt som det finns skäl att anta att det krävs en inte obetydlig övergångsperiod innan den lagstiftningen kan träda i kraft. Mot denna bakgrund är den enda möjliga lösningen att ändra övergångsbestämmelserna och göra polisdatalagen tillämplig på de fingeravtrycksregister som i dag förs med stöd av Datainspektionens tillstånd.

Den bestämmelse om direktåtkomst som föreslås ligger i linje med förslaget till ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Enligt det förslaget bemyndigas regeringen att meddela föreskrifter om att utländska myndigheter får medges direktåtkomst till fingeravtrycks- och signalementsregister om det följer av internationella åtaganden (4 kap. 13 §; se Ds 2007:43 s. 223 f. och 464).

Förutsättningarna för direktåtkomst och behandling i svenska register bör regleras i lagen om internationellt polisiärt samarbete och i förordning. På samma sätt som när det gäller tillgång till DNA-profiler (se avsnitt 7.7.1) ska sökningarna i fingeravtrycksregister kanaliseras via det svenska kontaktstället. I avsnitt 7.13 diskuteras vilken myndighet som ska vara svenskt kontaktställe.

Svenska myndigheters möjligheter att göra sökningar i andra staters fingeravtrycksregister behandlas i avsnitt 7.11.

7.9.2 Den fortsatta handläggningen

Om det kan konstateras en överensstämmelse mellan fingeravtrycksuppgifter regleras frågan om vilka personuppgifter och vilken ytterligare information som får översändas av den tillfrågade medlemsstatens lagstiftning, inkluderande reglerna om rättslig hjälp i brottmål (artikel 10). Det innebär att samma regler som gäller för informationsutbyte i allmänhet tillämpas vid bedömningen av i vilken omfattning namn och andra personuppgifter ska översändas. Eftersom all handläggning i detta skede faller utanför rådsbeslutet aktualiseras inte några lagändringar.

7.10 Fordonsuppgifter

Förslag: Ändamålsbestämmelsen i lagen om vägtrafikregister utvidgas i syfte att andra stater ska kunna ges direktåtkomst till vissa uppgifter i registret, för att förebygga och utreda brott, undersöka vissa överträdelser eller för att upprätthålla allmän säkerhet. En förutsättning är att uppgiftsinhämtandet sker i enlighet med en internationell överenskommelse som riksdagen har godkänt. Uppgifterna får endast avse vem som är ett fordons ägare och innehavare samt uppgifter om själva fordonet.

Skälen för förslaget: Genom sina nationella kontaktställen ska medlemsstaterna kunna göra automatiska sökningar i varandras register över fordonsuppgifter. Kontaktställena ska ha direkt tillgång till vissa uppgifter, om behandlingen sker för att förebygga och utreda brott, för undersökning av vissa överträdelser samt för att upprätthålla allmän säkerhet (artikel 12.1). De uppgifter som ska utbytas är uppgifter om vem som är ägare och innehavare av fordon samt uppgifter om fordonet. Rådsbeslutet får i denna del uppfattas så att angivna registeruppgifter omfattas i den utsträckning de förekommer i de nationella registren. Endast fordonets fullständiga chassinummer eller fullständiga registreringsnummer får användas för sökning i andra medlemsstaters register. I kap. 3 i bilagan till genomförandebestämmelserna finns detaljerade regler för utbytet av sådana uppgifter.

Redan i dag förekommer ett omfattande informationsutbyte mellan de europeiska myndigheter som ansvarar för nationella register över fordonsuppgifter. Informationsutbytet sker till viss del automatiskt genom EUCARIS (se avsnitt 5.4.2). Utbytet rör i första hand uppgifter om tillverkare och bilmodell, men systemet indikerar också om ett fordon är anmält stulet. Uppgifterna har stor betydelse bl.a. för ursprungskontroller samt fiskala och

administrativa kontroller. Informationsutbytet omfattar emellertid inte polisiärt samarbete.

Transportstyrelsen (tidigare Vägverket, se prop. 2008/09:31) för vägtrafikregistret, som innehåller uppgifter om fordon och deras ägare. Lagstiftningen om vägtrafikregister genomgår för närvarande en översyn, bl.a. avseende ändamålen för registret och behandlingen av personuppgifter i detta (se avsnitt 6.4.3).

Vägtrafikregistret innehåller bl.a. uppgifter om motordrivna fordon och släpfordon och om ägare till dessa (6 § 1 lagen [2001:558] om vägtrafikregister). Med ägare jämställs innehavaren, när det är fråga om fordon som innehas på grund av kreditköp med förbehåll om återtaganderätt, eller med nyttjanderätt för en bestämd tid om minst ett år (4 §). Den som på detta sätt innehar ett fordon enligt avbetalnings- eller leasingkontrakt behandlas alltså i registreringshänseende som fordonsägare (prop. 2000/01:95 s. 77 f.). De uppgifter som finns i vägtrafikregistret får anses motsvara det uppgiftsutbyte som rådsbeslutet förutsätter, dvs. uppgifter om ägare och innehavare samt uppgifter om fordonet.

I 5 § lagen om vägtrafikregister regleras för vilka ändamål personuppgifterna i registret får behandlas. Det är inte tillåtet att behandla uppgifterna för andra ändamål än de som uttryckligen anges. Registret får tillhandahålla personuppgifter för verksamhet för vilken staten eller en kommun ansvarar enligt lag eller annan författning bl.a. i fråga om fordonsägare och olika typer av tillstånd att föra fordon (5 § 1–5). Rådsbeslutets bestämmelser om tillhandahållande av uppgifter till andra medlemsstater ryms inte i ändamålsbestämmelserna i den paragrafen. Den måste således ändras. Ändringen görs lämpligen genom att man inför ytterligare en punkt i 5 § som upptar det nya ändamålet. Ändamålsbestämmelserna styr emellertid också möjligheterna till direktåtkomst. I 8 § lagen om vägtrafikregister föreskrivs att direktåtkomst till personuppgifter får medges endast för sådana ändamål som anges i 5 § 1–3 samma lag. Även bestämmelsen om direktåtkomst i 8 § måste därför ändras.

Eftersom lagen om vägtrafikregister enbart reglerar övergripande frågor förutsätter genomförandet av rådsbeslutet även ändringar i förordningen (2001:650) om vägtrafikregister (vägtrafikregisterförordningen).

Vägtrafikregisterförordningen innehåller bl.a. närmare bestämmelser om direktåtkomst (4 kap. 3–5 §§). Direktåtkomsten begränsas genom en hänvisning till den ovan redovisade ändamålsbestämmelsen i 5 § lagen om vägtrafikregister (4 kap. 3 § vägtrafikregisterförordningen med däri gjord hänvisning till 8 § lagen om vägtrafikregister). Genom den föreslagna ändringen av 5 § lagen om vägtrafikregister kommer möjligheten till direktåtkomst att omfatta alla de uppgifter rådsbeslutet föreskriver. Direktåtkomst förutsätter att behandlingen av personuppgifter är tillåten enligt personuppgiftslagen. Vidare får direktåtkomst till vägtrafikregistret medges först sedan Transportstyrelsen har försäkrat sig om att behörighets- och säkerhetsfrågorna är lösta på ett sätt som är tillfredsställande ur integritetssynpunkt (4 kap. 4 § vägtrafikregisterförordningen). Nu redovisade krav riskerar inte att hamna i konflikt med rådsbeslutet och dess reglering avseende dataskydd och datasäkerhet.

Enligt 4 kap. 12 § vägtrafikregisterförordningen får uppgifter ur vägtrafikregistret lämnas ut till en utländsk myndighet om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt. Bestämmelsen, som är tillämplig på rådsbeslutet, är sekretessbrytande.

Svenska myndigheters möjligheter att behandla uppgifter i andra medlemsstaters fordonsregister redovisas i det följande avsnittet.

7.11 Svenska sökningar i andra staters register

Förslag: De grundläggande förutsättningarna för att det svenska kontaktstället ska få söka efter uppgifter i andra staters register regleras i lagen om internationellt polisiärt samarbete. Närmare bestämmelser meddelas i förordning.

Skälen för förslaget: Informationsutbytet med stöd av rådsbeslutet bygger på att kontaktstället, inte enskilda myndigheter, inhämtar uppgifter i andra medlemsstaters DNA-, fingeravtrycks- och fordonsregister. Vi återkommer i avsnitt 7.13 till vilken myndighet som ska fungera som svenskt kontaktställe och förmedla uppgifter med stöd av rådsbeslutet.

Rådsbeslutet förutsätter, som tidigare nämnts, att automatiska sökningar och automatiska jämförelser kan genomföras i andra medlemsstaters register. Uppgifter i DNA-registren får enligt rådsbeslutet, oavsett sökförfarande, enbart behandlas ”i samband med brottsutredningar” (artikel 3 och 4). Automatisk sökning av fingeravtrycksuppgifter får förekomma både i brottsförebyggande och brottsutredande syfte (artikel 9). Utbyte av uppgifter i fordonsregister får ske för nyssnämnda ändamål, men även för att undersöka vissa andra överträdelser och för att upprätthålla allmän säkerhet (artikel 12). Det krävs regler som gör det möjligt för tjänstemän vid det svenska kontaktstället att genomföra sökningar och behandla uppgifter i utländska register för nu angivna ändamål. Eftersom det svenska rättssystemet bygger på att alla överträdelser av strafflagstiftning utreds i brottmålsförfarande finns det dock inget behov av att, som i vissa andra länder, kunna inhämta uppgifter för alternativa utredningsförfaranden.

Huvudprinciperna för sökning och automatiska jämförelser i utländska register bör läggas fast i lag, lämpligen lagen om internationellt polisiärt samarbete, medan den närmare regleringen bör ske i förordning (se avsnitt 7.3). I den mån det krävs behandling i svenska register för att genomföra sökning i utländska

register, t.ex. för att få fram en DNA-profil som ska jämföras med uppgifter i andra staters DNA-register, måste detta också ha stöd i lagstiftningen.

Enligt rådsbeslutet är det den ansökande medlemsstatens lagstiftning som, med de begränsningar som följer av rådsbeslutet, avgör om en sökning får ske i en annan medlemsstats register (se artikel 3.1, 4.1 och 9.1). De möjligheter rådsbeslutet ger att söka i andra medlemsstaters register påverkar därför inte vilka behandlingar som är tillåtna enligt svensk rätt. Det innebär t.ex. att analysresultat från DNA-prov som tagits från andra personer i en brottsutredning än de som är misstänkta för brott, t.ex. målsägande, inte får jämföras med uppgifter i andra staters DNA-register (se avsnitt 5.2). Däremot kan en sökning i en annan medlemsstats register innebära att tillgång ges till uppgifter som inte skulle kunna behandlas i svenska register. Så kan t.ex. vara fallet om längre gallringsfrister tillämpas i den andra medlemsstaten för personer som frikänts för brott eller om man registrerar uppgifter rörande någon som enligt svensk lag inte är straffmyndig.

Beträffande fingeravtryck bör påpekas att svenska myndigheters behandling av sådana uppgifter för att förebygga brott enligt polisdatalagen enbart får ske i förundersökningar eller särskilda undersökningar inom kriminalunderrättelseverksamheten. Detta torde täcka de praktiska behov som finns att behandla fingeravtrycksuppgifter. Enligt förslaget till ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet kommer personuppgifter i bl.a. fingeravtrycksregister att kunna behandlas även i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet (2 kap. 5 §; se Ds 2007:43 s. 130 f. och 409 f.). I avvaktan på att en ny reglering träder i kraft finns det inte skäl att nu ändra ändamålen för behandling av personuppgifter i fingeravtrycksregister.

7.12 Sekretess

Bedömning: Det krävs inga nya sekretessregler för att uppfylla rådsbeslutets bestämmelser.

Skälen för bedömningen: Andra staters rätt att behandla uppgifter i svenska register kan inte baseras på offentlighetsprincipen, eftersom den har annat syfte och uppgifterna dessutom kan omfattas av sekretess. För att Sverige ska uppfylla kraven i rådsbeslutet måste säkerställas att sekretessregleringen inte utgör hinder mot att uppgifterna lämnas ut till kontaktställena i andra medlemsstater i Europeiska unionen.

De uppgifter som enligt rådsbeslutet får utbytas kan bl.a. omfattas av sekretess till skydd för brottsbekämpningen enligt 5 kap. 1 § sekretesslagen. Sådan sekretess gäller t.ex. för uppgift som hänför sig till förundersökning i brottmål, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller att den framtida verksamheten skadas om uppgiften röjs. Sekretessen gäller i varierande grad i pågående, avslutade och nedlagda förundersökningar. Bestämmelsen omfattar dock inte utredningar i ärenden om internationell rättslig hjälp i brottmål, där i stället 5 kap. 7 § kan vara tillämplig. Sekretess enligt 5 kap. 1 § sekretesslagen omfattar även annan verksamhet vid brottsbekämpande myndigheter än brottsutredning, exempelvis brottsförebyggande åtgärder. Om åtal väcks upphör normalt sekretessen enligt den paragrafen.

Vidare kan sekretess gälla för uppgift om enskilds personliga och ekonomiska förhållanden i utredning enligt reglerna om förundersökning i brottmål (9 kap. 17 § första stycket 1 sekretesslagen). Den paragrafen har ett vidare tillämpningsområde än 5 kap. 1 §. Sekretessen gäller bl.a. för användning av straffprocessuella tvångsmedel och internationell rättslig hjälp i brottmål. Sekretess till skydd för enskild gäller också för uppgifter hos brottsbekämpande myndigheter för deras verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott (9 kap. 17 § för-

sta stycket 4). Sekretessen gäller vidare för uppgifter i vissa register som förs av Rikspolisstyrelsen med stöd av polisdatalagen eller som annars behandlas där med stöd av samma lag (9 kap. 17 § första stycket 6). DNA-register och fingeravtrycksregister tillhör de register som faller under bestämmelsen.

En sekretessbelagd uppgift får röjas för en utländsk myndighet eller mellanfolklig organisation bl.a. om utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning (1 kap. 3 § tredje stycket sekretesslagen). Enligt 7 § polisdatalagen får uppgifter lämnas ut till en utländsk myndighet eller en mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Regeringen får vidare meddela föreskrifter om att uppgifter på begäran får lämnas till polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott. En sådan bestämmelse finns i 18 § polisdataförordningen (1999:81).

I de fall där det finns en regel om direktåtkomst till uppgifter i ett register anses uppgiften i princip vara utlämnad redan när direktåtkomsten medges. Detta gäller oavsett om myndigheten faktiskt tar del av uppgiften eller inte. Det betyder att en förutsättning för att direktåtkomst ska kunna medges är att åtkomsten antingen endast avser offentliga uppgifter eller enbart omfattar uppgifter som får lämnas ut till mottagaren med stöd av någon sekretessbrytande bestämmelse (se Ds 2007:43 s. 228).

Eftersom uppgiftslämnande enligt rådsbeslutet uppfyller kravet i 7 § polisdatalagen kan direktåtkomst medges. För sådana uppgifter som andra medlemsstater får tillgång till genom direktåtkomst utgör sekretessregleringen således inget hinder.

Uppgifter som rör allmän ordning och säkerhet omfattas i betydligt mindre utsträckning av sekretess och i de fallen ska uppgiftslämnandet inte ske automatiserat. Sekretessregleringen bör därför inte heller i de fallen utgöra något hinder. I de fall där det finns en bindande förpliktelse att lämna information är 7 § polisdatalagen tillämplig. Däremot måste en sekretessprövning

göras i det enskilda fallet när uppgifter lämnas på svenskt initiativ utan någon sådan förpliktelse.

De aktuella uppgifterna i vägtrafikregistret är offentliga.

7.13 Nationellt kontaktställe

Förslag: Begreppet kontaktställe definieras i lagen om internationellt polisiärt samarbete. Rikspolisstyrelsen utses till svenskt kontaktställe för att förmedla förfrågningar med stöd av rådsbeslutet. Kontaktstället ska både hantera registersökningar, uppgifter som utbyts i samband med större evenemang med gränsöverskridande verkningar och uppgifter som utbyts i syfte att förebygga terroristbrott. Frågor som rör det praktiska arbetet regleras i förordning.

Skälen för förslaget: Enligt rådsbeslutet ska ett nationellt kontaktställe utses för förmedling av uppgifter som utbyts mellan medlemsstaterna (artikel 6.1, 11.1, 12.2, 15 och 16.3). Kontaktställets befogenheter regleras i nationell rätt.

DNA- och fingeravtrycksregister hanteras av Rikspolisstyrelsen och SKL. Styrelsen är personuppgiftsansvarig för förande av registren och ansvarar för driften av fingeravtrycksregister. SKL sköter i egenskap av personuppgiftsbiträde DNA-registren och hanterar således det praktiska arbetet kring dessa. Myndigheten gör också analysen av DNA-prov och bedömningarna av DNA-profiler. Det praktiska arbetet kring fingeravtryck hanteras till stor del av SKL, men också av Nationella fingeravtrycksavdelningen vid Rikskriminalpolisen.

Kontaktstället ska fungera som en länk för uppgiftsutbytet med andra medlemsstater i Europeiska unionen och ansvara för sökningar i andra medlemsstaters register. Rikspolisstyrelsen har redan nu i uppdrag att vara nationell enhet för den internationella kriminalpolisorganisationen (Interpol) och den europeiska polisbyrån (Europol). Styrelsen ansvarar vidare för den natio-

nella delen av Schengens informationssystem (SIS) och är nationell kontaktpunkt för SIS genom Sirenekontoret (2 § andra stycket förordningen [1989:773] med instruktion för Rikspolisstyrelsen). Det elektroniska utbytet enligt rådsbeslutet förutsätts ske genom kommunikationsnätet Testa II, vilket Rikspolisstyrelsen redan arbetar i vid sina internationella kontakter. Vidare kan anmärkas att Finland har pekat ut Centralkriminalpolisen som kontaktställe för sina kontakter enligt rådsbeslutet (se RP 243/2006 rd s. 17 f.).

Det sagda talar för att Rikspolisstyrelsen är mest lämpad att fungera som svenskt kontaktställe för förmedling av DNA-profiler och uppgifter i fingeravtrycksregister. Uppgiften kan regleras i förordning. Det är emellertid viktigt att framhålla att även om styrelsen pekas ut som svenskt kontaktställe förändrar detta inte SKL:s roll vare sig när det gäller analysarbetet eller rollen som personuppgiftsbiträde för DNA-registren. Hur det praktiska arbetet närmare ska bedrivas och på vilket sätt uppgifterna fördelas kräver inte någon lagstiftning.

Ett nationellt kontaktställe ska också utses för förmedling av uppgifter ur vägtrafikregistret (artikel 12.2). Vägtrafikregistret förs som tidigare nämnts av Transportstyrelsen. Det skulle därför kunna te sig naturligt att utse styrelsen till nationellt kontaktställe. Syftet med informationsutbytet är emellertid att förebygga och utreda brott, att undersöka vissa andra överträdelser samt att upprätthålla allmän säkerhet. Uppgiften som nationellt kontaktställe måste därför läggas på en brottsbekämpande myndighet. Redan en förfrågan från en utländsk myndighet kan omfattas av sekretess till skydd för utländsk brottsbekämpning. Sekretess enligt 5 kap. 7 § sekretesslagen förekommer endast hos brottsbekämpande myndigheter. Det finns därför skäl att utse Rikspolisstyrelsen till nationellt kontaktställe också vid informationsutbyte avseende fordonsuppgifter.

Nationella kontaktställen ska utses också för övrigt informationsutbyte enligt rådsbeslutet (artikel 15 och 16.3). I propositionen om godkännande av rådsbeslutet konstaterade regeringen att samma organ som utses till nationellt kontaktställe för för-

medling av DNA- och fingeravtrycksuppgifter lämpligen bör utses till nationellt kontaktställe också för förmedling av uppgifter i samband med större evenemang (prop. 2007/08:83 s. 27). Det finns inte skäl att nu göra någon annan bedömning.

Det lämpligaste är givetvis att endast ha ett nationellt kontaktställe. Rikspolisstyrelsen bör därför pekas ut som kontaktställe också för uppgifter som utbyts mellan staterna i syfte att förebygga terroristbrott. Visserligen är det främst en uppgift för Säkerhetspolisen att bekämpa terrorism (se 2 § andra stycket förordningen [2002:1050] med instruktion för Säkerhetspolisen). Säkerhetspolisen för också det s.k. SÄPO-registret som bl.a. har till ändamål att underlätta spaning i syfte att bekämpa terrorism (32 § polisdatalagen). Från effektivitetssynpunkt finns det emellertid fördelar med ett enda kontaktställe för informationsutbyte enligt rådsbeslutet. Eftersom Säkerhetspolisen ingår i Rikspolisstyrelsen kan styrelsen se till att den information som ska vidarebefordras till Säkerhetspolisen tas om hand på lämpligt sätt.

En viktig uppgift för kontaktstället blir att ansvara för de sökningar i utländska register som rådsbeslutet ger möjlighet till. Särskilda tjänstemän ska utpekas för uppgiften (se vidare avsnitt 7.19.2).

Som framhållits tidigare ska regelverket om rättslig hjälp tilllämpas för det fortsatta informationsutbytet sedan det konstaterats att en DNA-profil eller ett fingeravtryck finns i något av de svenska registren. Det innebär bl.a. att de fortsatta kontakterna inte ska gå via kontaktstället.

7.14 Informationsutbyte vid större evenemang

7.14.1 Översändande av personuppgifter till en annan stat

Förslag: Det svenska kontaktställets skyldighet att vid större nationella eller utländska evenemang med gränsöverskridande verkningar översända personuppgifter till en annan stat, i syfte att förebygga brott och ordningsstörningar, regleras i förordning.

Skälen för förslaget: Rådsbeslutet föreskriver skyldighet för medlemsstaterna att på begäran eller på eget initiativ översända personuppgifter till en annan medlemsstat i samband med ”större evenemang med gränsöverskridande verkningar” (artikel 14.1). Informationsutbytet ska syfta till att förebygga brott eller att upprätthålla allmän ordning och säkerhet. För att personuppgifter ska sändas över krävs att det på grundval av lagakraftvunna domar eller andra fakta finns skäl att anta att de personer som uppgifterna avser kommer att begå brott vid det berörda evenemanget eller att de utgör ett hot mot ordningen och säkerheten. Det ska alltså finnas en konkret grund för misstanken om att personen kommer att begå brott eller störa ordningen. Även underrättelseuppgifter kan aktualiseras, men dessa måste i så fall bygga på konkreta fakta.

De uppgifter som översänds får enbart användas för att förebygga brott och upprätthålla ordningen vid det utpekade evenemanget. Användningsbegränsningar behandlas i avsnitt 7.17.4.

Rådsbeslutet exemplifierar ”större evenemang med gränsöverskridande verkningar” med betydande idrottsevenemang och Europeiska rådets möten. Andra tänkbara evenemang är vissa internationella sammankomster som behandlar kontroversiella frågor och större möten i ett NATO-organ, om dessa i det enskilda fallet kan antas leda till brott eller allvarliga ordningsproblem. Liknande problem vid statsbesök eller besök av internationellt välkända personer är andra exempel. Artikeln bör uppfattas

så att den avser såväl nationella som utländska evenemang, så länge evenemanget i fråga är gränsöverskridande. Informationsutbyte förefaller aktualiseras främst vid sådana tilldragelser som berör ett stort antal personer och som kan antas beröra flera länders polisverksamhet.

I samband med vissa större evenemang utbyts redan i dag uppgifter mellan stater om personer som förekommer i polisens eller andra brottsbekämpande myndigheters register. Detta samarbete utvecklas genom det uppgiftsutbyte som rådsbeslutet föreskriver. Behandlingen av sådana uppgifter regleras i huvudsak av polisdatalagen, när den sker som ett led i polisens verksamhet. Bestämmelserna i lagen om belastningsregister kan också aktualiseras. Bestämmelser om utlämnande av uppgifter till en utländsk myndighet finns bl.a. i 7 § polisdatalagen, 11 § lagen om belastningsregister och 24 § förordningen (1999:1134) om belastningsregister (se även prop. 2008/09:18 s. 24 f. angående utbyte av uppgifter ur kriminalregister). Gällande rätt medger alltså att uppgifter översänds till andra medlemsstater i enlighet med rådsbeslutet, men föreskriver ingen sådan skyldighet som rådsbeslutet får anses förutsätta (se regeringens tolkning av artikel 14 i prop. 2007/08:83 s. 26). En sådan skyldighet bör därför införas genom en ny bestämmelse i förordning. Någon särskild reglering för det fall utbytet skulle avse uppgifter som omfattas av sekretess krävs inte, eftersom de tidigare nämnda bestämmelserna är sekretessbrytande (se avsnitt 7.12).

7.14.2 Översändande av icke personrelaterade uppgifter till en annan stat

Förslag: Det svenska kontaktställets skyldighet att vid större nationella eller utländska evenemang med gränsöverskridande verkningar översända andra uppgifter än personuppgifter, om dessa bedöms vara nödvändiga för att förebygga brott eller hot mot ordningen och säkerheten vid evenemanget, regleras i förordning.

Skälen för förslaget: I samband med större evenemang med gränsöverskridande verkningar är medlemsstaterna också skyldiga att sända andra medlemsstater nödvändiga *icke personrelaterade* uppgifter (artikel 13). I fråga om sådana uppgifter krävs endast att uppgifterna är nödvändiga för att förebygga brott eller upprätthålla ordning och säkerhet vid evenemanget. Den bedömningen får göras i varje enskilt fall. Det kan t.ex. röra sig om uppgifter att en grupp icke identifierade personer, som misstänks vara våldsbenägna, kan komma att bevista evenemanget. Ett annat exempel är allmän information om vissa utpekade grupper som kan komma att störa evenemanget, t.ex. underrättelseinformation som inte innehåller några personuppgifter.

Bestämmelsen är formulerad som en obligatorisk förpliktelse för medlemsstaterna att kunna sända varandra sådana uppgifter, samtidigt som den hänvisar till att uppgiftsutbytet ska ske i enlighet med nationell rätt i den översändande staten. Regeringen har tidigare tolkat bestämmelsen så att den föreskriver en skyldighet för svenska myndigheter att översända uppgifter till andra länder i samband med större evenemang, men att medlemsstaterna råder över den närmare utformningen av reglerna och de begränsningar som ska gälla (se prop. 2007/08:83 s. 25). Det saknas skäl att nu göra någon annan bedömning. Även skyldigheten att sända staterna andra uppgifter än personuppgifter kräver en ny bestämmelse, vilken kan tas in i förordning. Någon

särskild reglering för det fall utbytet skulle avse uppgifter som omfattas av sekretess krävs inte (se avsnitt 7.12).

7.14.3 Utplåning av personuppgifter som översänts till Sverige

Förslag: Skyldigheten att utplåna personuppgifter som erhållits från en annan stat inom ramen för Prümsamarbetet regleras i förordning.

Skälen för förslaget: Rådsbeslutet begränsar inte bara medlemsstaternas rätt att behandla sådana uppgifter som översänts från en annan medlemsstat inför ett större evenemang (se avsnitt 7.14.1), utan begränsar också hur länge uppgifterna får bevaras. Enligt artikel 14.2 ska personuppgifter som översänts i samband med större evenemang med gränsöverskridande verkningar utplånas omedelbart när syftet med mottagandet har uppnåtts eller inte längre kan uppnås. Under alla förhållanden ska personuppgifterna utplånas senast inom ett år.

Eftersom huvudsyftet med informationsutbytet är att förebygga och förhindra brott och allvarliga ordningsstörningar ligger det i sakens natur att de flesta personuppgifter som översänts ska utplånas när evenemanget är över. Varken polisdatalagen eller någon annan nu aktuell författning innehåller någon bestämmelse som motsvarar den i rådsbeslutet. Det kan visserligen hävdas att huvudregeln är att personuppgifter som inte längre behövs för sitt ursprungliga ändamål ska gallras (13 § polisdatalagen), men som utvecklas närmare i det följande (avsnitt 7.18) finns det ändå utrymme för att bevara vissa uppgifter. Det bör därför i förordning föreskrivas att nu aktuella personuppgifter ska utplånas senast efter ett år.

7.15 Bistånd

Förslag: Skyldigheten att, inom ramen för Prümrådssamarbetet, bistå en annan stat, i syfte att förhindra brott och upprätthålla ordning och säkerhet vid större evenemang och liknande viktiga händelser, katastrofer och allvarliga olyckor med gränsöverskridande verkningar, regleras i förordning. Det svenska kontaktstället ska så tidigt som möjligt underrätta andra berörda stater om situationen och förmedla väsentlig information om denna. Rikspolisstyrelsen ska samordna nödvändiga polisiära åtgärder och kunna besluta om att ställa tjänstemän, specialister och rådgivare samt nödvändig utrustning till en annan stats förfogande.

Skälen för förslaget: Medlemsstaterna är skyldiga att, enligt nationell rätt, på olika sätt bistå varandra vid större evenemang med gränsöverskridande verkningar och liknande händelser, katastrofer och allvarliga olyckor (artikel 18). Biståndet begränsas genom att syftet ska vara att förhindra brott och upprätthålla allmän ordning.

En form av bistånd är att så tidigt som möjligt informera andra medlemsstater om situationer med gränsöverskridande verkningar samt förmedla väsentliga uppgifter om dem (artikel 18 a). Denna skyldighet kan t.ex. aktualiseras vid evenemang där man kan förutse att det finns risk för våldshandlingar eller allvarliga ordningsstörningar.

Medlemsstaterna är vidare skyldiga att i situationer med gränsöverskridande verkningar genomföra och samordna nödvändiga polisiära åtgärder på sitt territorium (artikel 18 b). I den mån det är möjligt ska också, på begäran av den berörda staten, tjänstemän, specialister och rådgivare samt nödvändig utrustning ställas till förfogande (artikel 18 c).

Skyldigheten att, inom ramen för Prümrådssamarbetet, på begäran bistå en annan stat vid större evenemang och liknande händelser, katastrofer och allvarliga olyckor begränsas till vad

som är tillåtet enligt svensk lagstiftning. I fråga om bistånd med tjänstemän, specialister, rådgivare och utrustning gäller den ytterligare begränsningen ”i den mån det är möjligt”. Trots dessa begränsningar får bestämmelsen betraktas som ett åliggande för Sverige att lämna bistånd till andra stater i de situationer som omfattas (prop. 2007/08:83 s. 31 f.), även om det inte är någon absolut skyldighet. Exempel på bistånd kan vara att polisfordon med särskild utrustning lånas ut eller att en polishelikopter med personal tillfälligt ställs till en annan stats disposition. Liknande skyldigheter förekommer i andra sammanhang, bl.a. grundade på bi- eller multilaterala avtal om räddningstjänst och miljöräddningstjänst till sjöss. Regeringen eller den myndighet regeringen bestämmer kan t.ex. enligt 9 kap. 1 § andra stycket lagen (2003:778) om skydd mot olyckor begära eller lämna internationellt bistånd vid räddningsinsatser enligt internationella överenskommelser som Sverige ingått. Bemyndigandet gäller enbart räddningsinsatser, vilket får anses motsvara rådsbeslutets begrepp katastrofer och allvarliga olyckor, men däremot inte bistånd vid större evenemang och liknande viktiga händelser. Det krävs därför en ny bestämmelse som reglerar förpliktelsen att på begäran bistå en annan stat i ordningshållande och brottsförebyggande syfte. Denna skyldighet kan regleras i förordning, liksom skyldigheten att samordna nödvändiga polisiära åtgärder i Sverige om det uppstår situationer med gränsöverskridande verkningar som direkt berör vårt land. Samordningsansvaret bör läggas på Rikspolisstyrelsen. Eftersom det inte på förhand går att förutse vilka samordningsbehov som kan aktualiseras och dessa kan komma att beröra flera polismyndigheter har Rikspolisstyrelsen en viktig samordningsfunktion. Styrelsen kan givetvis när det är lämpligt överlämna till en polismyndighet att ansvara för samordningen, t.ex. i de fall där endast en polismyndighet berörs.

Bistånd med personalresurser kan i enstaka fall innebära att svenska tjänstemän behöver föra ut skjutvapen och ammunition ur Sverige (artikel 19.1). Enligt 6 § lagen (1992:1300) om krigsmateriel krävs som huvudregel tillstånd för att föra ut krigsmate-

riel ur Sverige. Krigsmateriel är enligt 1 § samma lag vapen, ammunition och annat för militärt bruk utformad materiel som enligt regeringens föreskrifter utgör krigsmateriel. I en bilaga till förordningen (1992:1303) om krigsmateriel förtecknas sådan materiel och dit kan också höra viss polisiär utrustning. Som regeringen konstaterat i propositionen om godkännande av Prümrådsbeslutet finns det för närvarande inget generellt undantag som ger svenska polismän rätt att medföra skjutvapen och ammunition till ett annat land (prop. 2007/08:83 s. 33). Skulle behov av detta uppkomma kan emellertid tillstånd meddelas efter en prövning i det enskilda fallet (6 § lagen om krigsmateriel). Det får anses vara tillräckligt att förlita sig på en sådan prövning.

Rådsbeslutet föreskriver som huvudregel att värdstaten ska ersätta de eventuella skador som orsakas av utländska tjänstemän som bistår en annan medlemsstat vid större evenemang, katastrofer och allvarliga olyckor (artikel 21.4). Vidare föreskrivs regressrätt för värdstaten i förhållande till den stat som tillhandahåller tjänstemännen, för skada som dessa orsakat genom grov oaktsamhet eller avsiktlig försummelse (artikel 21.5). Skadeståndsansvar kan därför aktualiseras endast i undantagsfall. Regressrätten är en fråga av mellanstatlig karaktär som inte direkt berör den skadelidande eller tredje man, eller påverkar deras möjligheter att få skadestånd. Mot den bakgrunden krävs ingen lagreglering.

7.16 Andra former av gränsöverskridande samarbete

Bedömning: Övriga bestämmelser i rådsbeslutet om gränsöverskridande polissamarbete föranleder inga lagstiftningsförslag inom ramen för detta uppdrag.

Skälen för bedömningen: I syfte att fördjupa det polisiära samarbetet innehåller rådsbeslutet en fakultativ reglering angående bistånd genom gemensamma patruller och gemen-

samma insatser. Den innebär att utländska tjänstemän kan ges rätt att tillsammans med en annan stats tjänstemän tjänstgöra uniformerade och beväpnade på den statens territorium (artikel 17 och 19). En stat kan också ge tjänstemän från andra stater rätt att utöva verkställande befogenheter på sitt territorium (artikel 17.2). Sådana befogenheter får dock endast utövas under överinsyn av och i regel i närvaro av värdstatens tjänstemän. Rådsbeslutet förskriver att andra medlemsstaters tjänstemän ska ha samma straffrättsliga ansvar och samma skydd som statens egna tjänstemän (artikel 20 och 22). Rådsbeslutet innehåller också allmänna bestämmelser om skadeståndsansvar (artikel 21).

Enligt det uppdrag som denna promemoria grundar sig på ska innehållet i de nu redovisade artiklarna utredas särskilt (Justitiedepartementet, dnr Ju2008/5996/P). Det är därför inte aktuellt att i detta sammanhang göra några ytterligare överväganden angående dessa artiklar.

7.17 Integritetsskydd

7.17.1 Allmänt om integritetsskyddet

Utbyte av information kan innebära risker för enskildas integritet. Det bör emellertid framhållas att det är stora skillnader mellan olika typer av uppgifter. Generellt sett är t.ex. uppgifter i vägtrafikregistret betydligt mindre integritetskänsliga än uppgifter i DNA-registren.

Informationsutbytet enligt rådsbeslutet påverkar inte det grundläggande integritetsskydd vid personuppgiftsbehandling som bl.a. polisdatalagen och personuppgiftslagen ger. Dessutom är det viktigt att erinra om att myndigheterna redan utbyter den typ av information som Prümrådsbeslutet tar sikte på (se vidare avsnitt 7.1.1). Det nya sättet att arbeta innebär därför i första hand att den som efterfrågar viss information snabbare får veta om det finns några uppgifter av intresse. Eftersom de mera integritetskänsliga uppgifterna inte kan hänföras till en identifierbar

person är risken att skada någon person genom oförsiktig eller felaktig behandling av uppgifterna i princip undanröjd. På samma sätt som i dag måste den stat som vill ha närmare uppgifter vända sig till den andra staten med en begäran om rättslig hjälp. Vidare innehåller rådsbeslutet bestämmelser om grundläggande dataskydd och användningsbegränsningar som syftar till att förstärka integritetsskyddet. Denna reglering behandlas närmare i det följande.

Det förhållandet att medlemsstaterna får tillgång till vissa uppgifter i varandras register innebär alltså inte i sig att riskerna för integritetsintrång ökar.

7.17.2 Grundläggande dataskyddsnivå

Bedömning: Den svenska lagstiftningen uppfyller rådsbeslutets krav på viss grundläggande dataskyddsnivå.

Skälen för bedömningen: Rådsbeslutet föreskriver att behandling av uppgifter som översänds eller har översänts minst ska motsvara den dataskyddsnivå som dataskyddskonventionen föreskriver (artikel 25 och avsnitt 6.2.2). Detta gäller all behandling av personuppgifter. Konventionens krav i fråga om översändande av uppgifter mellan stater och om ömsesidigt bistånd mellan staterna ska beaktas. För de stater som inte redan utbyter information med stöd av Prümfördraget är det en förutsättning för att uppgifter ska få översändas att dataskyddsbestämmelserna har införlivats nationellt (artikel 25.2 och 25.3). Även principerna i Europarådets ministerkommittés rekommendation R (87) 15 av den 17 september 1987 ska iakttas (se vidare avsnitt 6.2.3).

Enligt rådsbeslutet ska samma dataskyddsnivå gälla oavsett om uppgifter behandlas automatiskt eller manuellt (artikel 25.1). Det framgår emellertid inte om detta skydd avser all manuell behandling av uppgifter eller om det bara gäller sådan behandling som sker i register. I andra rättsakter, och i svensk rätt, omfattar

dataskyddet enbart sådan manuell behandling som sker i register (se prop. 2007/08:83 s. 40). Det finns inte anledning att tolka rådsbeslutet på annat sätt. Det innebär att rådsbeslutet i detta hänseende motsvaras av regleringen i personuppgiftslagen (5 § andra stycket personuppgiftslagen). De allmänna skyddsreglerna i 9 § första stycket personuppgiftslagen – som bl.a. föreskriver en lagenlig och korrekt behandling av personuppgifter, men också att uppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål samt inte får behandlas för något ändamål som är oförenligt med det för vilket de samlades in – har i tidigare lagstiftningsärenden bedömts uppfylla den allmänna skyddsnivå som dataskyddskonventionen kräver (se bl.a. prop. 1999/2000:64 s. 147 f.). I propositionen om godkännande av rådsbeslutet har samma bedömning gjorts (prop. 2007/08:83 s. 40). Det krävs således inga lagstiftningsåtgärder, eftersom svensk rätt redan uppfyller rådsbeslutets krav på att det ska finnas en grundläggande dataskyddsnivå.

7.17.3 Datasäkerhet och annat dataskydd

Bedömning: Den svenska lagstiftningen uppfyller rådsbeslutets krav på datasäkerhet och annat dataskydd.

Skälen för bedömningen: Översändande och mottagande myndigheter ska enligt rådsbeslutet vidta åtgärder så att personuppgifter skyddas effektivt mot oavsiktlig eller otillåten utplåning, oavsiktlig förlust, obehörig tillgång, obehörig eller oavsiktlig ändring och obehörigt offentliggörande (artikel 29.1). När det gäller direktåtkomst och det automatiska sökförfarandet fastställs olika säkerhetsåtgärder i genomförandebeslutet, som exempelvis vad som ska gälla i fråga om kryptering.

Allmänna krav på säkerhet vid behandling av personuppgifter regleras i 31 § personuppgiftslagen. Enligt den bestämmelsen ska den personuppgiftsansvarige bl.a. vidta lämpliga tekniska och

organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Bestämmelsen är tillämplig också på enskilda register eftersom det i stort sett saknas avvikande regler. Datainspektionen har gett ut allmänna råd om säkerhet för personuppgifter. Vidare finns särskilda bestämmelser i 3, 5 och 6 §§ arkivlagen (1990:782) om hur arkivhandlingar och arkiv ska hanteras, vilka är av betydelse för bevarande av förundersökningar (prop. 1997/98:44 s. 92). Det bör också nämnas att Europolkonventionen och Schengenkonventionen innehåller en reglering som motsvarar den i rådsbeslutet och att man vid genomförandet av dessa konventioner har bedömt att de allmänna skyddsreglerna i personuppgiftslagen uppfyller de säkerhetskrav som ställs (prop. 1996/97:164 s. 46, 1999/2000:64 s. 148 och 2006/07:33 s. 11). Samma bedömning har gjorts i propositionen om godkännande av Dataskyddsrambeslutet (prop. 2008/09:16 s. 52 f.). Det finns inte skäl att göra någon annan bedömning i detta lagstiftningsärende. Eftersom svensk rätt uppfyller kraven på datasäkerhet och annat dataskydd i rådsbeslutet krävs inte några lagändringar i detta avseende.

7.17.4 Användningsbegränsningar

Förslag: Skyldigheten enligt lagen om internationellt polisiärt samarbete för svenska myndigheter att iaktta användningsbegränsningar som en annan stat har förelagt utvidgas, så att även uppgifter som har översänts i syfte att upprätthålla allmän ordning och säkerhet omfattas.

En ny bestämmelse införs som ger svenska myndigheter möjlighet att i enskilda fall ställa villkor för användandet av uppgifter som lämnas till en annan stat eller en mellanfolklig organisation, om villkor krävs med hänsyn till enskilds rätt eller från allmän synpunkt. Sådana villkor får inte strida mot svenska internationella åtaganden.

Skälen för förslaget

Villkor för användning av uppgifter som mottas

Rådsbeslutet begränsar staternas rätt att behandla personuppgifter som har översänts. En begränsning ligger i den grundläggande ändamålsbestämmelsen. Behandling hos en mottagande stat får bara ske för de syften för vilka uppgifterna har översänts (artikel 26.1). Behandling för andra syften är tillåten endast om det finns förhandstillstånd från den medlemsstat som administrerar uppgifterna, dvs. den stat som översänder eller gör uppgifterna tillgängliga. Vidare begränsas kretsen av myndigheter som får hantera översända uppgifter till behöriga myndigheter, dvs. brottsbekämpande myndigheter och domstolar (artikel 27). För att en utländsk uppgift ska få lämnas vidare till en annan myndighet krävs att den översändande myndigheten på förhand lämnar tillstånd till detta och att den mottagande medlemsstatens lagstiftning inte hindrar att uppgifterna behandlas av annan myndighet.

Rådsbeslutet begränsar alltså möjligheten att behandla uppgifter och vissa av artiklarna får därför betraktas som en användningsbegränsande reglering (se bl.a. prop. 1990/91:131 s. 25 och 2008/09:16 s. 40).

Svenska myndigheter som inom ramen för polisiärt samarbete får uppgifter från en annan stat är skyldiga att följa eventuella villkor som begränsar användningen, oavsett vad som annars är föreskrivet i lag eller annan författning. Bestämmelser om detta finns i 3 § lagen om internationellt polisiärt samarbete. Regleringen omfattar dock enbart uppgifter som överlämnats för användning i underrättelseverksamhet om brott, vid utredning av brott eller i ett rättsligt förfarande med anledning av brott. Utbyte av uppgifter med stöd av rådsbeslutet kan emellertid också komma att ske för andra syften än de nu nämnda. Uppgifter ska t.ex. kunna översändas för upprätthållande av allmän ordning och säkerhet vid vissa större evenemang med gränsöverskridande verkningar (artikel 13 och 14, se avsnitt 7.14). För att svenska

myndigheter ska vara skyldiga att iaktta de användningsbegränsningar som föreskrivs i rådsbeslutet beträffande uppgifter som översänts i syfte att upprätthålla ordning och säkerhet krävs att 3 § lagen om internationellt polisiärt samarbete ändras.

Villkor för användning av uppgifter som översänds

Rådsbeslutet aktualiserar också svenska myndigheters möjlighet att på motsvarande sätt ställa villkor för uppgifter som översänds till eller görs tillgängliga för brottsbekämpande myndigheter i andra medlemsstater (artikel 16.4). I dag kan villkor för användningen ställas vid internationell rättslig hjälp (5 kap. 2 § LIRB) och internationellt tullsamarbete (2 kap. 7 § lagen om internationellt tullsamarbete), men däremot inte vid internationellt polissamarbete. Eftersom det kan finnas lika starka skäl att ställa upp villkor för användningen av uppgifter som lämnas till en utländsk stat som ett led i internationellt polissamarbete behöver regleringen göras heltäckande. Förfrågningar som görs av t.ex. Europol kan också aktualisera behov av användningsbegränsande villkor. Även i det informationsutbyte som sker med stöd av förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen kan en svensk myndighet behöva ställa upp villkor för användningen av uppgifter som utbyts (Ds 2008:72 s. 63 f.). Eftersom behovet av att kunna ställa sådana villkor är generellt bör det införas en regel om detta i lagen om internationellt polissamarbete. En svensk myndighet som översänder uppgifter eller gör uppgifter tillgängliga för en annan stat eller en mellanfolklig organisation ska således få ställa upp villkor för användningen. Begreppet mellanfolklig organisation anses omfatta Europeiska unionens institutioner. Villkor som står i strid med våra internationella åtaganden får givetvis inte ställas upp. Det innebär att om en viss överenskommelse inte tillåter att informationsutbytet begränsas genom villkor för användningen måste det respekteras. Den myndighet som har ställt ett villkor för användningen ska även kunna medge

undantag från villkoret. Någon särskild bestämmelse om detta krävs dock inte.

7.18 Korrigering och bevarande av personuppgifter

Förslag: I förordning meddelas regler om i vilka situationer personuppgifter som inom ramen för Prümsamarbetet har översänts från eller gjorts tillgängliga av en annan stat ska utplånas, spärras eller märkas samt under vilka förutsättningar märkning ska kunna avlägsnas.
Bedömning: Rådsbeslutets reglering i fråga om rättelse kräver ingen lagstiftningsåtgärd.

Skälen för förslagen och bedömningen

Innehållet i rådsbeslutet

Rådsbeslutet anvisar flera metoder för att säkerställa att uppgifter som utbyts är korrekta och aktuella (artikel 28). Häri ingår särskilda bestämmelser om hur länge uppgifter får bevaras och i vilka fall de ska utplånas.

Felaktiga uppgifter eller uppgifter som inte borde ha översänts ska antingen *rättas* eller *utplånas* (artikel 28.1 och 28.3). Skyldigheten omfattar både sådana uppgifter som har översänts av en myndighet i annan stat och uppgifter som en svensk myndighet har inhämtat genom sökning i en annan medlemsstats register.

När utplåning aktualiseras ska hänsyn tas till om det finns skäl att anta att utplåning skulle skada den berörda personens intressen (artikel 28.3). Om så är fallet ska uppgifterna i stället *spärras*, dvs. förses med anteckning om att uppgifterna inte får användas fritt. Uppgifter som har spärrats får därefter endast översändas eller användas i det syfte som ledde till att uppgif-

terna spärrades i stället för att utplånas. Det närmare förfarandet vid spärrning ska enligt rådsbeslutet regleras nationellt.

Om en berörd person bestrider att personuppgifterna är korrekta och det inte är möjligt att fastställa om så är fallet, kan uppgifterna på begäran av den personen i stället *märkas* i enlighet med nationell rätt (artikel 28.2). Sådan märkning får, enligt regler i nationell rätt, avlägsnas endast om den person som uppgifterna rör har lämnat sitt medgivande eller efter beslut av en behörig domstol eller en oberoende myndighet som ansvarar för övervakningen av dataskyddet. Märkning hindrar, i motsats till spärrning, inte att uppgifterna används (artikel 24 c).

När det gäller vilken av de anvisade metoderna som ska väljas, får rådsbeslutet uppfattas så att delvis felaktiga uppgifter normalt ska rättas. I fråga om uppgifter som i sin helhet är felaktiga, som inte borde ha översänts eller mottagits, som inte längre behövs för det syfte för vilka de översändes eller som inte längre får bevaras därför att den tidsfrist som fastställts för lagring av uppgifterna i den översändande staten har löpt ut (artikel 28.3), är det inte lika givet hur rådsbeslutet ska tolkas. Bestämmelser av motsvarande slag har i tidigare lagstiftningsärenden tolkats så, att den personuppgiftsansvarige avgör vilken metod som ska användas för korrigering (prop. 1997/98:44 s. 87). Typiskt sett anses myndigheter inte, i strid med offentlighetsprincipen och arkivlagstiftningen, ha rätt att vidta åtgärder som innebär att uppgifter i allmänna handlingar raderas. Det vanliga är att felaktiga uppgifter rättas och kompletteras. Uppgifter som inte längre behövs kan ofta gallras.

Utplåning av uppgifter

Utplåning av uppgifter kan, som framgått ovan, aktualiseras av fyra olika skäl enligt bestämmelserna i artikel 28. Rådsbeslutet föreskriver vidare att när ett kontaktställe i en annan stat har gjort en sökning i vägtrafikregistret, ska de fordonsuppgifter som har översänts från den staten utplånas när den automatiska

sökningen har besvarats och någon ytterligare behandling inte är nödvändig för registrering (artikel 26.3).

I rådsbeslutet används genomgående begreppet utplåning. I den engelska texten används begreppet ”delete”. Det finns skäl att inledningsvis uppehålla sig något vid terminologin.

När personuppgifter utplånas innebär det att uppgifterna förstörs eller behandlas på annat sätt, så att de inte längre kan användas eller återskapas. Syftet är alltså att göra personuppgifterna oåtkomliga för alltid. Begreppet utplåna förekommer i personuppgiftslagen (9 och 26 §§). I arkivsammanhang används i stället begreppet ”gallring” (2 kap. tryckfrihetsförordningen och 10 § arkivlagen). Gallring kan innebära förstörande (t.ex. att pappershandlingar kastas). Även byte av datamedium räknas i vissa sammanhang som gallring, trots att informationen finns kvar. I bl.a. 27 kap. 24 § rättegångsbalken används uttrycket ”förstöra”. Den paragrafen reglerar hur upptagningar och uppteckningar som härrör från användning av hemliga tvångsmedel ska hanteras. Det finns således inte några entydiga begrepp. I detta sammanhang är det dock mest naturligt att välja samma uttryck som i rådsbeslutet, dvs. utplåna.

Vad gäller frågan om hur rådsbeslutet förhåller sig till svensk rätt kan vidare följande konstateras. Att utplåna personuppgifter på den grunden att *uppgifterna är felaktiga* motsvaras delvis av skyldigheten enligt 9 § första stycket h personuppgiftslagen att vidta alla rimliga åtgärder för att utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Däremot finns det inte någon regel om utplåning av *uppgifter som inte borde ha sänts*. Möjligen kan skyldigheten att utplåna felaktigt översända uppgifter betraktas som ett generellt användningsbegränsande villkor. I 3 § lagen om internationellt polisiärt samarbete regleras hur sådana villkor ska behandlas. Eftersom bestämmelserna om användningsbegränsningar syftar till begränsningar av ett mer aktivt förfarande, dvs. att använda erhållna uppgifter, är dock en sådan tolkning tveksam (jfr regeringens bedömning i prop. 2007/08: 83 s. 47). Dessutom aktualiseras villkoret först i efterhand, vilket också stäm-

mer mindre väl med regleringen angående användningsbegränsningar. När det däremot gäller *uppgifter som överskridit den längsta tillåtna tiden för bevarande* rör det sig om ett villkor som är känt redan vid översändandet och som därmed kan sägas utgöra ett villkor för att uppgifterna ska få användas. Därmed torde svenska myndigheter vara skyldiga att utplåna uppgifterna enligt 3 § lagen om internationellt polisiärt samarbete. Den svenska lagstiftningen kan därför anses uppfylla rådsbeslutets krav i sistnämnda hänseende.

Enligt rådsbeslutet ska vidare *uppgifter utplånas om de i och för sig översänts korrekt, men inte längre är nödvändiga för det syfte för vilket de översändes*. Enligt 13 § polisdatalagen ska personuppgifter gallras om de inte längre behövs för sitt ändamål. För uppgifter i förundersökningar gäller i stället bestämmelserna i arkivlagen. Arkivlagen föreskriver dock inte någon allmän skyldighet att gallra uppgifter.

För de av polisens register som berörs av rådsbeslutet finns särskilda gallringsregler. För uppgifter i fingeravtrycksregister gäller Datainspektionens föreskrifter om gallring, vilka i sak överensstämmer med 31 § polisdatalagen.[44] Enligt föreskrifterna ska uppgifter i fingeravtrycksregistret om en misstänkt person gallras när förundersökning eller åtal mot personen läggs ned eller när åtal ogillas. Uppgifterna får dock besvaras längre om andra uppgifter om den registrerade behandlas med stöd av 10 eller 11 § polisdatalagen. När sistnämnda uppgifter gallras ska även uppgifterna i fingeravtrycksregistret gallras. Om den registrerade döms ska uppgifterna i registret gallras senast vid den tidpunkt då uppgifterna gallras ur belastningsregistret.

Polisdatalagen innehåller olika gallringsbestämmelser för de tre DNA-registren. Uppgifter i *DNA-registret* ska gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret. Uppgifter i *utredningsregistret* ska gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller

[44] Datainspektionens beslut den 1 december 2005, Dnr 698-2005, meddelat med stöd av punkten 2 i övergångsbestämmelserna till polisdatalagen samt 6 och 18 §§ datalagen.

när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade godkänner ett strafföreläggande som avser enbart böter. Det innebär att uppgifterna i utredningsregistret förs över till DNA-registret om den misstänkte döms till annan påföljd än böter och att uppgifterna tas bort om någon lagföring inte sker, åtalet ogillas eller påföljden stannar vid böter. Uppgifter i *spårregistret* ska gallras senast trettio år efter registreringen.

Även om gällande lagstiftning innehåller gallringsbestämmelser som till vissa delar motsvarar rådsbeslutets krav ger den utrymme för att uppgifter kan bevaras även efter det att syftet med behandlingen har tillgodosetts. Detta gäller bl.a. uppgifter i förundersökningar som i stället gallras enligt arkivlagstiftningen. Den nuvarande regleringen ska ses mot bakgrund av den grundlagsskyddade offentlighetsprincipen och allmänhetens rätt att ta del av allmänna offentliga handlingar. För att uppfylla kraven i rådsbeslutet bör man därför också reglera kravet på att utplåna uppgifter som inte längre behövs för det ändamål för vilket de översändes.

För att få en samlad reglering bör en bestämmelse införas som ger tydligt stöd för att utplåna översända personuppgifter i alla de nu aktuella situationerna. Regleringen bör kunna tas in i förordning, eftersom den till stor del utgör en specialreglering för Prümrådssamarbetet och därmed enbart kompletterar befintliga bestämmelser.

Spärrning

Ibland kan det ligga i den registrerades intresse att personuppgifter bevaras, trots att de enligt huvudregeln i rådsbeslutet skulle ha utplånats. Detta beaktas i rådsbeslutet genom att det ges möjlighet att i stället spärra uppgifter, om utplåning skulle innebära skada för den person uppgifterna rör (artikel 28.3).

Eftersom spärrning utgör ett alternativ till utplåning kan spärrning aktualiseras i samtliga situationer där uppgifter ska

utplånas. Det innebär att uppgifter kan spärras om de är felaktiga, inte borde ha översänts, inte längre behövs för det ursprungliga ändamålet eller när den översändande statens längsta tillåtna tid för bevarande har löpt ut. För att uppfylla kraven i rådsbeslutet måste en särskild regel om spärrning införas i förordning.

Ett beslut om spärrning begränsar möjligheterna till fortsatt behandling. Spärrning torde dock inte hindra att uppgifterna lämnas ut enligt bestämmelserna i 2 kap. tryckfrihetsförordningen.

Märkning

Som redovisats ovan kan *märkning* aktualiseras på begäran av den person som uppgifterna rör, om personen bestrider uppgifternas korrekthet och det inte är möjligt att fastställa om de är korrekta eller felaktiga (artikel 28.2). Sådan märkning får, enligt närmare regler i nationell rätt, avlägsnas endast om den person som uppgifterna rör har lämnat sitt medgivande eller efter beslut av en behörig domstol eller en oberoende myndighet som ansvarar för övervakningen av dataskyddet.

Det finns inga tillämpliga regler om märkning i svensk rätt. I propositionen om godkännande av rådsbeslutet konstaterade regeringen att det är oklart i vilken mån Sverige måste införa ett märkningsförfarande för personuppgifter som översänds eller mottas med stöd av rådsbeslutet. Regeringen fann att medlemsstaterna visserligen är skyldiga att reglera märkningsförfarandet, men att de själva råder över den närmare utformningen av reglerna och vilka begränsningar som ska gälla (prop. 2007/08:83 s. 47).

Det finns inte skäl att frångå regeringens preliminära bedömning att man måste reglera märkning av uppgifter i syfte att värna enskildas integritetsskydd. Därför ska en regel införas som möjliggör märkning av personuppgifter på begäran av den person som uppgifterna rör, om den berörda personen bestrider person-

uppgifternas korrekthet och det inte kan fastställas om uppgifterna är riktiga eller inte. Ett beslutet om märkning förutsätter en viss utredning om uppgiftens riktighet. Går det att fastställa att uppgiften är korrekt ska givetvis ingen märkning ske och om den är felaktig ska den enligt huvudregeln rättas eller utplånas.

Om uppgifter har märkts ska märkningen som huvudregel kunna avlägsnas endast efter medgivande av den person som uppgiften rör. Märkning ska emellertid också kunna avlägsnas efter särskilt beslut.

Rådsbeslutet förutsätter alltså att den berörda personen endera lämnar sitt medgivande till åtgärden eller att en domstol eller oberoende tillsynsmyndighet fattar beslut i frågan. Eftersom märkning tillkommer på den enskildes initiativ är det uppenbart att personen i fråga knappast är intresserad av att märkningen avlägsnas om det senare visar sig att den omstridda uppgiften är korrekt. Det måste därför finnas möjlighet att få märkningen avlägsnad mot den enskildes vilja. Märkningen bör för det första kunna tas bort om en domstol i ett lagakraftvunnet beslut har funnit att den omstridda uppgiften är korrekt eller felaktig, dvs. om uppgiftens korrekthet har kunnat fastställas. En sådan bedömning skulle t.ex. kunna göras mot bakgrund av uttalanden i en brottmålsdom om faktiska förhållanden eller annat. Vidare bör ett beslut om märkning kunna upphävas av Datainspektionen på begäran antingen av den berörda personen eller den myndighet som förfogar över uppgiften. En särskild regel om detta bör införas.

Enligt 51 § personuppgiftslagen finns det en generell möjlighet att hos allmän förvaltningsdomstol, dvs. länsrätt, överklaga en tillsynsmyndighets beslut enligt den lagen. Eftersom det saknas regler om märkning i personuppgiftslagen kan nämnda bestämmelse dock inte anses vara tillämplig på Datainspektionens beslut i fråga om märkning (se bl.a. Ds 2008:81 s. 98 f.). Att det med stöd av allmänna förvaltningsrättsliga principer anses finnas möjlighet att överklaga tillsynsmyndigheters beslut torde inte vara tillräckligt för att uppfylla förpliktelserna i rådsbeslutet. Det

bör därför införas en särskild regel om överklagande av Datainspektionens beslut i en fråga om märkning.

Märkningsförfarandet i sin helhet kräver alltså särskild reglering. Denna kan tas in i förordning.

Rättelse

Som framhållits inledningsvis i detta avsnitt ska felaktiga personuppgifter kunna rättas eller utplånas (artikel 28.1). I 28 § personuppgiftslagen regleras möjligheten att kräva att felaktiga personuppgifter rättas. Paragrafen gäller vid behandling av uppgifter i polisens verksamhet och i vägtrafikregistret. Bestämmelsen om rättelse i personuppgiftslagen kan emellertid åberopas enbart av fysiska personer. Det är oklart om rådsbeslutet har motsvarande begränsning. Eftersom informationsutbytet (med undantag för vissa fordonsuppgifter) har tydlig inriktning på uppgifter om fysiska personer torde nämnda begränsning sakna praktisk betydelse. Någon lagstiftningsåtgärd krävs därför inte i denna del.

Sammanfattande slutsatser

Rådsbeslutet kräver ny reglering av såväl utplånande som spärrning och märkning. I förordning bör föreskrivas att personuppgifter som har översänts från, eller gjorts tillgängliga av, en annan stat ska *utplånas* om

1. uppgifterna är felaktiga,
2. uppgifterna inte borde ha översänts,
3. uppgifterna i och för sig har översänts och mottagits korrekt, men inte längre är nödvändiga för det ändamål för vilket de översändes, eller
4. den längsta tid för bevarande som en utländsk myndighet med stöd av nationell lagstiftning har angett i samband med översändandet har överskridits.

Uppgifterna ska i stället *spärras* om utplåning av uppgifterna skulle skada den som uppgifterna rör.

Dessutom ska personuppgifter kunna *märkas* på begäran av den som uppgifterna rör, om denne bestrider att uppgifterna är korrekta och deras korrekthet inte kan fastställas.

Det bör framhållas att det knappast kommer att bli vanligt att reglerna om spärrning och märkning aktualiseras, bl.a. därför att rådsbeslutets informationsutbyte i huvudsak rör ett fåtal typer av personuppgifter. Det kan dock inte uteslutas att det exempelvis finns oklarheter angående identiteten på någon vars DNA-profil eller fingeravtryck har registrerats eller att det pågår en tvist angående på vem ett visst fordon rätteligen ska vara registrerat.

7.19 Kontroll och tillsyn

7.19.1 Underrättelse- och informationsskyldighet

Förslag: Det införs en skyldighet för kontaktstället att underrätta mottagaren av uppgifterna i en annan stat om att översända uppgifter visat sig vara felaktiga eller inte borde ha översänts. Kontaktstället ska också på begäran informera en översändande stat om behandlingen av de översända uppgifterna och om de resultat som har erhållits. Dessa skyldigheter regleras i förordning.

Bedömning: Gällande lagstiftning uppfyller rådsbeslutets krav på information till en registrerad person om vilka uppgifter om vederbörande som är eller har varit föremål för behandling.

Skälen för förslaget och bedömningen

Kontaktställets skyldigheter

Översändande stat och mottagande organ har en ömsesidig underrättelseskyldighet, om det visar sig att uppgifterna var felaktiga eller om de inte borde ha översänts (artikel 28.1). Vidare ska en mottagande stat på begäran informera den översändande staten om behandlingen av de översända uppgifterna och om de resultat som har erhållits (artikel 32).

Skyldigheten att informera om att översända uppgifter är felaktiga, eller inte borde ha översänts, är ett av flera moment i rådsbeslutet som syftar till att säkerställa att de uppgifter som utbyts är korrekta och aktuella (se även avsnitt 7.18). Underrättelseskyldigheten, som bör åvila kontaktstället, bör därför komma till direkt uttryck i författning men kan regleras i förordning.

Frågan är vilken myndighet i den andra staten som ska underrättas. Ett alternativ är att enbart underrätta den andra statens kontaktställe. Ett annat är att underrätta både kontaktstället och andra mottagare som man känner till. Det sistnämnda alternativet torde vara det som står bäst i överensstämmelse med tankarna bakom rådsbeslutet och hänsynen till enskilda. Om det är känt att en viss myndighet har mottagit uppgiften bör denna så snart som möjligt få kännedom om att uppgiften är felaktig eller inte borde ha översänts. Däremot kan det inte krävas att svenska myndigheter undersöker vilken eller vilka myndigheter som eventuellt har fått uppgifterna från det utländska kontaktstället.

För att det svenska kontaktstället ska kunna fullgöra sin skyldighet bör den myndighet som ansvarar för den översända informationen åläggas att underrätta kontaktstället, om det visar sig att översända uppgifter är felaktiga eller inte borde ha översänts.

Vidare krävs det en bestämmelse om det svenska kontaktställets skyldighet att på begäran av ett kontaktställe i en stat informera om behandlingen av de översända uppgifterna och om de

resultat som har erhållits. Någon direkt motsvarighet till denna skyldighet finns inte i svensk lagstiftning, även om det i flera författningar finns regler som ålägger svenska myndigheter att informera översändande stat om hur översända uppgifter har använts. Även denna skyldighet kan regleras i förordning.

Information till enskilda

Enligt artikel 31 i rådsbeslutet har en registrerad person bl.a. rätt att på begäran informeras om de uppgifter om vederbörande som är eller har varit föremål för behandling. De närmare formerna för informationen, däribland frågan i vilken utsträckning sekretess kan begränsa rätten till information, regleras nationellt. Rådsbeslutet föreskriver att den registrerade ska få del av informationen utan oskäliga avgifter, i en förståelig form och utan oacceptabla dröjsmål. Informationen ska omfatta åtminstone uppgifternas ursprung, mottagare eller kategori av mottagare, det avsedda ändamålet med behandlingen och, när så krävs i nationell lagstiftning, dess rättsliga grund.

I 23–27 §§ personuppgiftslagen finns generella bestämmelser om information till den registrerade. Bestämmelserna är tillämpliga på behandling av personuppgifter i polisens verksamhet och i vägtrafikregistret, eftersom det varken i polisdatalagen eller i lagen om vägtrafikregister finns några särregler.

Från integritetssynpunkt är 26 § personuppgiftslagen mycket viktig. Berörda personer har som huvudregel rätt att få information om de uppgifter som finns registrerade om dem. Var och en som ansöker om det har rätt att en gång om året gratis få information från den personuppgiftsansvarige om vilka personuppgifter som behandlas, varifrån de har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare uppgifterna lämnats. Rätten till information gäller dock inte om uppgifterna omfattas av sekretess eller tystnadsplikt (27 § personuppgiftslagen). Eftersom rådsbeslut medger att rätten till

information begränsas i enlighet med nationell lagstiftning behövs det inte några lagändringar i detta avseende.

7.19.2 Behörighet att genomföra sökningar

Förslag: Rikspolisstyrelsen ska ange vilka tjänstemän som får genomföra automatiska sökningar i andra staters register med stöd av rådsbeslutet. Detta regleras i förordning.

Bedömning: Inget hindrar att förteckningar över behöriga tjänstemän på begäran lämnas ut till tillsynsmyndigheter eller till andra stater som deltar i Prümrådssamarbetet.

Skälen för förslaget och bedömningen: Rådsbeslutet föreskriver att de tjänstemän som ska få genomföra automatiska sökningar och automatiska jämförelser i andra medlemsstaters databaser ska ha särskilt bemyndigande (artikel 30.2 a). En förteckning över dessa tjänstemän ska på begäran lämnas ut till tillsynsmyndigheterna och till övriga medlemsstater.

Rådsbeslutets begränsning av kretsen av tjänstemän som får genomföra automatiska sökningar och jämförelser kan i och för sig betraktas som en sådan skyddsåtgärd som avses i 31 § personuppgiftslagen. För att svensk rätt med säkerhet ska uppfylla rådsbeslutets förpliktelser bör det emellertid av en uttrycklig bestämmelse framgå att kretsen av tjänstemän som ska kunna genomföra automatiska sökningar med stöd av rådsbeslutet ska begränsas. En lämplig ordning är att kontaktstället, dvs. Rikspolisstyrelsen, genom särskilda beslut pekar ut vilka tjänstemän som har sådan behörighet och ansvarar för den dokumentation som på begäran ska lämnas till tillsynsmyndigheter och andra medlemsstater. Detta kan regleras i förordning.

Det finns inte några sekretessregler eller andra bestämmelser som hindrar att en förteckning över sådana tjänstemän överlämnas till tillsynsmyndigheter eller till andra medlemsstater. Rådsbeslutets krav i denna del är därmed uppfyllt.

7.19.3 Tillsyn

Förslag: Datainspektionen utses till tillsynsmyndighet enligt rådsbeslutet, vilket rådets generalsekretariat ska underrättas om. I förordning meddelas bestämmelser om tillsynsmyndighetens särskilda uppgifter enligt rådsbeslutet och dess möjlighet att utföra kontroller, att begära vissa upplysningar av myndigheter i andra stater som deltar i Prümrådssamarbetet och att anmoda dataskyddsmyndigheter i sådana stater att genomföra nödvändiga inspektioner.

Skälen för förslaget: Enligt rådsbeslutet ska staternas dataskyddsmyndigheter eller, i förekommande fall, de rättsliga myndigheterna i medlemsstaten, övervaka utbytet av personuppgifter ur ett rättsligt perspektiv (artikel 30.5). Var och en ska hos en sådan myndighet, i enlighet med nationell rätt, kunna ansöka om att få lagligheten av personuppgiftsbehandlingen granskad. Myndigheterna ska också genom stickprov kontrollera lagligheten. Sådana kontroller ska även utföras av de registreringsskyldiga organen. Resultaten av kontrollerna ska för granskningsändamål förvaras hos dataskyddsmyndigheterna i 18 månader (artikel 30.5). Därefter ska de omedelbart utplånas. En dataskyddsmyndighet ska kunna anmoda en sådan myndighet i en annan medlemsstat att utföra kontroller i enlighet med sina nationella befogenheter. Samarbete ska vidare bl.a. kunna ske genom utbyte av relevant information (artikel 30.5).

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen (2 § personuppgiftsförordningen). För sin tillsyn har Datainspektionen rätt att på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter (43 § personuppgiftslagen). Inom ramen för tillsynen kan alltså bl.a. besök och egeninitierade granskningar göras (prop. 1997/98:44 s. 102).

Det är naturligt att Datainspektionen utses till tillsynsmyndighet för personuppgiftsbehandling som utförs med stöd av rådsbeslut, på samma sätt som inspektionen har den rollen när det gäller annan personuppgiftsbehandling inom polisen. Inspektionens allmänna befogenheter regleras i personuppgiftslagen och personuppgiftsförordningen. De särskilda uppgifter som myndigheten ska fullgöra enligt rådsbeslutet bör regleras i förordning. Uppdraget som tillsynsmyndighet bör också föranleda en ändring i myndighetens instruktion, t.ex. genom ett tillägg i 2 § förordningen (2007:975) med instruktion för Datainspektionen.

Ansvaret för tillsynen delas enligt rådsbeslutet mellan de berörda nationella dataskyddsmyndigheterna. Rådsbeslutet bör uppfattas så att Datainspektionen har ansvaret för tillsynen över behandling i de svenska registren och för sökningar som det svenska kontaktstället utför i andra medlemsstaters register.

På anmodan av en dataskyddsmyndighet i en annan stat som deltar i Prümrådssamarbetet ska tillsynsmyndigheten utföra inspektioner om detta är nödvändigt för samarbetet. Även om Datainspektionen har generell möjlighet att utföra inspektioner som ett led i sin tillsyn bör den direkta skyldigheten att agera på en annan stats begäran komma till uttryck i författning, men den kan regleras i förordning. Rådsbeslutets bestämmelser om förvaring och utplåning av kontrollresultat och skyldigheten att översända uppgifter om kontrollresultat till en dataskyddsmyndighet i en annan medlemsstat bör regleras på samma sätt. Likaså bör tillsynsmyndighetens rätt att anmoda en myndighet i en annan medlemsstat att genomföra nödvändiga inspektioner för att kontrollera behandlingen av personuppgifter som härrör från Sverige, och möjligheten att begära de uppgifter som rör behandlingen, regleras. Datainspektionen avgör själv de närmare formerna för tillsynen och samarbetet med andra dataskyddsmyndigheter.

Vid sidan av Datainspektionen har Säkerhets- och integritetsskyddsnämnden vissa tillsynsuppgifter enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Nämnden

har tillsyn över Säkerhetspolisens behandling av uppgifter enligt polisdatalagen. Enskilda har möjlighet att vända sig till nämnden och begära särskild kontroll. Tillsynen utövas bl.a. genom inspektioner (prop. 2006/07:133 s. 68 f.). Nämndens tillsynsuppgifter påverkas inte av rådsbeslutet.

Enligt artikel 19 i genomförandebeslutet ska rådets generalsekretariat underrättas om att Datainspektionen är tillsynsmyndighet enligt rådsbeslutet.

7.19.4 Registreringsskyldighet

Förslag: Skyldigheten att för kontrolländamål registrera vad som översänds respektive mottas med stöd av Prümrådssamarbetet på annat sätt än genom direktåtkomst samt den övriga registreringsskyldighet som föreskrivs i rådsbeslutet regleras i förordning. Registreringsskyldigheten ska åvila kontaktstället och det organ som administrerar databasen.

Skälen för förslagen

Rådsbeslutet föreskriver skyldighet att för kontrolländamål registrera både sådana uppgifter som har översänts eller mottagits på annat sätt än genom direktåtkomst och uppgifter som erhålls genom automatisk sökning eller automatisk jämförelse. Skyldigheten gäller dels för kontaktstället, dels för det organ som administrerar databasen.

För att det ska vara möjligt att i efterhand kontrollera sökningarna är medlemsstaterna skyldiga att vid varje *icke-automatiskt* översändande eller mottagande av personuppgifter föra register som visar hur de översända uppgifterna har behandlats (artikel 30.1). Av registreringen ska framgå skälet till översändandet, vilka uppgifter som har översänts och när det skedde, namn eller annan beteckning på det sökande organet och vem

som administrerar databasen. Registreringsskyldigheten åvilar både det sökande organet och den som administrerar databasen.

I fråga om *automatiska sökningar* och *automatiska jämförelser* i ett register som förs av en annan medlemsstat ska registreringen ge uppgift om sökningen eller jämförelsen lett till träff eller inte, vilka uppgifter som översänts och exakt när detta skedde samt namn eller annan beteckning på det sökande organet och den som administrerar databasen (artikel 30.2). Registreringsskyldigheten åvilar både det sökande organet och den som administrerar databasen. Det sökande organet ska dessutom ange syftet med sökningen eller jämförelsen och vilken tjänsteman som har beslutat om denna.

Den som är registreringsskyldig ska, utan dröjsmål och senast fyra veckor efter det att begäran kom in, delge den berörda medlemsstatens dataskyddsmyndigheter de registrerade uppgifterna (artikel 30.3). Den andra staten får endast använda uppgifterna för att övervaka dataskyddet och garantera datasäkerheten. Uppgifterna ska lagras i två år (artikel 30.4). När lagringstiden har löpt ut, ska uppgifterna utan dröjsmål utplånas.

Den noggrant reglerade registreringsskyldigheten ska ses mot bakgrund av att man inför direktåtkomst till vissa uppgifter. Direktåtkomsten innebär att kontrollen av att sökningarna eller jämförelserna har varit korrekta alltid måste ske i efterhand. En betydande del av registreringsskyldigheten torde med fördel kunna skötas automatiskt. Det gäller t.ex. registrering av när uppgifter har översänts eller mottagits, vilka uppgifter det rör sig om, namn eller annan beteckning på den sökande samt uppgift om vem som administrerar databasen.

Registreringsskyldigheten kan regleras i förordning. Den bör begränsas till de uppgifter som är obligatoriska enligt rådsbeslutet. Skyldigheten att för kontrolländamål lagra registrerade uppgifter i två år, liksom skyldigheten att därefter utplåna uppgifterna, bör regleras på samma sätt.

Även om Rikspolisstyrelsen enligt 22 § polisdatalagen för de svenska DNA-registren sköts den praktiska hanteringen av SKL i egenskap av personuppgiftsbiträde. Rikskriminalpolisen, som är

en del av Rikspolisstyrelsen, ansvarar för registrering och kvalitetssäkring av fingeravtryck, medan SKL sköter en stor del av arbetet med analys och jämförelser. Det bör därför ankomma på Rikspolisstyrelsen att, om det behövs, meddela närmare föreskrifter för registreringen.

När det gäller vägtrafikregistret utbyts uppgifter enbart genom direktåtkomst. Avser utbytet personuppgifter (ägare och innehavare av fordon) är Rikspolisstyrelsen registreringsskyldig i egenskap av kontaktställe (se avsnitt 7.13) och Transportstyrelsen i egenskap av administratör för registret. Som framgått ovan är det något färre uppgifter som ska registreras vid direktåtkomst.

Sammanfattningsvis krävs det bestämmelser som återspeglar skyldigheten att för kontrolländamål registrera uppgifter som har översänts eller mottagits både genom direktåtkomst och på annat sätt. Registreringsskyldigheten åvilar kontaktstället och det organ som administrerar databasen (om det inte är samma organ). Det krävs också en särskild regel om gallring av de registrerade uppgifterna.

7.20 Rätten att överklaga och begära skadestånd

Bedömning: Den svenska lagstiftningen uppfyller rådsbeslutets krav i fråga om berörda personers rätt att överklaga och begära skadestånd för felaktig behandling av personuppgifter.

Skälen för bedömningen

Innehållet i rådsbeslutet

Medlemsstaterna ska säkerställa att personer, vars rätt till dataskydd har kränkts, har möjlighet att överklaga hos en oavhängig domstol eller hos en oberoende tillsynsmyndighet och att personen kan kräva skadestånd eller annan ersättning (artikel 31.1).

Förfarandet för att hävda dessa rättigheter och skälen till eventuella begränsningar följer nationell rätt i den medlemsstat där personen hävdar sina rättigheter. Rådsbeslutet hänvisar till de rättigheter som föreskrivs i artikel 6.1 i Europakonventionen. Enligt den bestämmelsen har en person, vid prövningen av hans eller hennes civila rättigheter och skyldigheter eller vid en anklagelse mot honom för brott, rätt till domstolsprövning inom skälig tid. Det centrala i bestämmelsen är tillgång till domstol och att prövningen uppfyller vissa rättsliga garantier.

Rätten att överklaga

Den svenska lagstiftningen lever redan upp till kraven på tillgång till rättsmedel i Europakonventionen och rådsbeslutet. Datainspektionen granskar som tillsynsmyndighet myndigheters behandling av personuppgifter, bl.a. efter anmälan från enskilda. Datainspektionens befogenheter enligt 43–47 §§ personuppgiftslagen gäller vid den behandling av personuppgifter som informationsutbytet omfattar. Datainspektionens beslut enligt personuppgiftslagen får överklagas till allmän förvaltningsdomstol, dvs. i första instans länsrätt. Enligt 52 § personuppgiftslagen får en myndighets beslut om information och rättelse, underrättelse till tredje man samt upplysningar till allmänheten överklagas till förvaltningsdomstol. Den paragrafen är tillämplig på polisens register, eftersom polisdatalagen inte innehåller någon från personuppgiftslagen avvikande regel om överklagande, och på polisens personuppgiftsbehandling i övrigt. När det gäller vägtrafikregistret föreskrivs i 34 § lagen om vägtrafikregister att bl.a. beslut om rättelse eller information enligt personuppgiftslagen överklagas hos länsrätten i Örebro län. Det finns således bestämmelser som ger möjlighet att överklaga felaktiga registreringar i alla de berörda registren och i polisens personuppgiftsbehandling i övrigt.

Eftersom den svenska lagstiftningen uppfyller rådsbeslutets krav i fråga om rätt att överklaga felaktig behandling av personuppgifter krävs inga lagändringar.

Skadestånd

Medlemsstaterna ska, som nyss nämnts, säkerställa att en person, som hävdar att uppgifter om honom eller henne är felaktiga eller har behandlats på ett otillbörligt sätt, har möjlighet att kräva skadestånd. En mottagande myndighet i en medlemsstat kan inte undgå skadeståndsansvar gentemot en enskild person genom att hävda att uppgifter som den staten har mottagit från en annan medlemsstat är felaktiga (artikel 31.2). Myndigheten kan däremot göra anspråk på ersättning från den översändande myndigheten (regressanspråk).

I 48 § personuppgiftslagen finns allmänna bestämmelser om enskildas möjlighet att kräva skadestånd för den kränkning av den personliga integriteten som en behandling av personuppgifter i strid med lagen har orsakat. Skadestånd kan komma i fråga vid varje brott mot lagen och ska utgå trots att ingen har skadats fysiskt eller ekonomiskt. Det krävs inte heller att den personuppgiftsansvarige har haft uppsåt att göra fel eller varit försumlig vid behandlingen. Den stränga regleringen tar sin utgångspunkt i lagens huvudsakliga syfte att skydda människor mot kränkning av den personliga integriteten (SOU 1997:39 s. 432 och prop. 1997/98:44 s. 106). Rätten till skadestånd gäller dock enbart fysiska personer. En juridisk person som anser att behandlingen av uppgifter vållat skada har möjlighet att vända sig till Justitiekanslern eller till allmän domstol och begära skadestånd av staten enligt allmänna regler.

Det finns inga särbestämmelser om skadestånd för sådan uppgiftsbehandling som sker i nu aktuella register eller vid polisens personuppgiftsbehandling i allmänhet. Personuppgiftslagens reglering rörande skadestånd omfattar därför även sådan behandling. I den utsträckning ersättningsfrågan inte berörs i per-

sonuppgiftslagen, t.ex. hur ersättningen för en skada ska beräknas, tillämpas de allmänna reglerna i skadeståndslagen.

Staternas skyldigheter vid regressanspråk är mellanstatliga och kräver därför ingen lagstiftningsåtgärd. Som regeringen tidigare framhållit kan det emellertid finnas anledning att i lämpligt sammanhang överväga att reglera formerna för handläggningen av sådana regresskrav (prop. 2008/09:16 s. 55).

Sammanfattningsvis uppfyller svensk rätt rådsbeslutets bestämmelser i fråga om skadestånd. Det krävs därför inte några lagstiftningsåtgärder.

7.21 Rådsbeslutets effekter på övriga brottsbekämpande myndigheter

Trots att vissa delar av rådsbeslutet enbart rör polisiära frågor, som upprätthållande av allmän ordning och säkerhet, bistånd med polisiära resurser vid större evenemang med gränsöverskridande verkningar och sökning i register som administreras av polisen, så berör rådsbeslutet också andra brottsbekämpande myndigheter.

Tullverket, Ekobrottsmyndigheten i dess polisverksamhet och i någon mån även Kustbevakningen och Skatteverkets brottsutredande enheter kommer att kunna dra fördel av möjligheten att utbyta sådan information som omfattas av rådsbeslutet. Även om Tullverkets och Kustbevakningens brottsbekämpande uppgifter enbart omfattar vissa i författning angivna brottstyper så har dessa myndigheter i princip samma uppgifter som polisväsendet i sin brottsbekämpande verksamhet. Kustbevakningens rätt att inleda och bedriva förundersökning är dock mycket begränsad. Detta utesluter emellertid inte att båda myndigheterna snabbt behöver kunna kontrollera vissa uppgifter. Det förekommer inte sällan nära samverkan mellan polisen och Tullverket eller Kustbevakningen i det brottsbekämpande arbetet. Självfallet kan det även i en sådan situation behövas ett snabbt informationsutbyte. Ett sådant exempel är att polisen, Tullverket

och Kustbevakningen samarbetar vid ett planerat ingripande i ett kustnära område och då bl.a. snabbt måste få tillgång till uppgifter om vem som innehar ett fordon som är registrerat i en annan stat. Genom rådsbeslutet förbättras informationsutbytet i förhållande till dagens ordning.

För Tullverket kan möjligheten att automatiskt söka efter uppgifter ur andra medlemsstaters DNA- och fingeravtrycksregister få betydelse när spår av det slaget har säkrats i en förundersökning om smugglingsbrott, men också i annan brottsbekämpande och brottsutredande verksamhet.

Samtliga brottsbekämpande myndigheter behöver också snabbare och enklare få tillgång till fler registeruppgifter, bl.a. mot bakgrund av den ökande gränsöverskridande brottsligheten. Direktåtkomst till andra medlemsstaters DNA-, fingeravtrycks- och fordonsuppgifter är därför av stor betydelse i den dagliga verksamheten.

När det blir aktuellt att utbyta information med stöd av rådsbeslutet ska detta praktiskt hanteras av Rikspolisstyrelsen i egenskap av nationellt kontaktställe. Detta gäller såväl svenska förfrågningar som framställningar från utländska myndigheter om information. Därför kommer övriga myndigheter inte att beröras av de ändringar som krävs för att möjliggöra sökningar i utländska register. Trots att kontakterna går via Rikspolisstyrelsen berörs emellertid den brottsbekämpande myndighet som har initierat en sökning eller mottagit information med stöd av rådsbeslutet av reglerna i detta, t.ex. när det gäller hur uppgifterna får användas och i vilka fall de ska utplånas.

De särskilda författningar om personuppgiftsbehandling som gäller för övriga brottsbekämpande myndigheter har betydande likheter med regleringen i polisdatalagen. Som konstaterats i propositionen om godkännande av dataskyddsrambeslutet ger alla dessa författningar samma grundläggande dataskydd (se prop. 2008/09:16 och avsnitt 4.3). De innehåller bl.a. bestämmelser om gallring, rättelse, blockering och utplåning. Personuppgiftslagens bestämmelser om information till den registrerade är tillämpliga.

Enligt 24 § förordningen om behandling av personuppgifter inom Kustbevakningen ska uppgifter som huvudregel gallras när de inte längre behövs med hänsyn till ändamålen med behandlingen. Motsvarande gäller för Skatteverkets brottsbekämpande verksamhet enligt 15 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar. Även för Tullverkets brottsbekämpande verksamhet finns en särskild gallringsregel, 27 § lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Enligt den paragrafen ska uppgifter som behandlas automatiserat i ett ärende som huvudregel gallras senast ett år efter det att ärendet avslutades. Bestämmelserna om gallring gäller inte förundersökningar.

Dessa gallringsbestämmelser uppfyller inte i alla delar kraven på utplånande i rådsbeslutet, då de lämnar visst utrymme att bevara uppgifter. Eftersom myndigheterna ska tillämpa de särskilda reglerna i lagen om internationellt polissamarbete på uppgifter som erhålls med stöd av rådsbeslutet krävs dock inga ändringar i deras lagstiftning om behandling av personuppgifter.

7.22 Rådsbeslutets effekter på Transportstyrelsen

Sedan flera år förekommer utbyte av fordonsinformation mellan medlemsstaterna i Europeiska unionen, bl.a. inom ramen för kommunikationsnätverket EUCARIS (se vidare avsnitt 5.4.2). Med stöd av EUCARIS kan uppgifter utbytas om tillverkare och bilmodell, typ av fordon, färg, vilken typ av bränsle fordonet använder och en statussignal som bl.a. indikerar om bilen är stulen eller skrotad. Rådsbeslutet föreskriver att direktåtkomsten till fordonsregister, utöver uppgifter om själva fordonet, också omfattar uppgifter om vem som är fordonets ägare och innehavare. Det innebär att ytterligare uppgifter kan utväxlas.

Eftersom rådsbeslutet syftar till utbyte av polisiär information förslås Rikspolisstyrelsen fungera som kontaktställe även för information från vägtrafikregistret. Detta ska bl.a. ses mot

bakgrund av att den information som utbyts kan omfattas av sekretess som inte är tillämplig i Transportstyrelsens verksamhet.

Lagstiftningen om vägtrafikregister är, som redovisats i avsnitt 6.4.3, föremål för en total översyn. De författningsändringar som genomförandet av rådsbeslutet kräver (se avsnitt 7.10) kommer sannolikt att påverkas av översynen, särskilt om denna leder till helt ny lagstiftning.

7.23 Rådsbeslutets tekniska krav

Genomförandet av rådsbeslutet kräver också att medlemsstaterna, dvs. ytterst de berörda myndigheterna, vidtar ett antal tekniska åtgärder med sina register, för att möjliggöra att andra medlemsstater får direktåtkomst till vissa uppgifter (se även avsnitt 9). Detta gäller framför allt automatiska sökningar och automatiska jämförelser, dvs. utbyte av uppgifter om DNA-profiler, fingeravtryck och fordon. I genomförandebeslutet föreskrivs bl.a. att vissa gemensamma tekniska specifikationer ska iakttas, att fastställda principer för uppgiftsutbytet måste följas samt att viss sökningskapacitet ska kunna upprätthållas. När det gäller dessa frågor föreskriver rådsbeslutet en genomförandetid på tre år. Det innebär att myndigheterna behöver ha fungerande tekniska lösningar som uppfyller kraven i rådsbesluten först i augusti 2011.

8 Norges och Islands associering till rådsbeslutet

Bedömning: Norges och Islands förväntade associering till rådsbeslutet bör föranleda att lagstiftningen utformas generellt, så att den inte enbart reglerar förhållandet till andra medlemsstater i Europeiska unionen.

Skälen för bedömningen: Norge och Island, som sedan tidigare ingår i Schengenområdet[45] men inte är medlemmar i Europeiska unionen, har förklarat att de önskar delta i samarbetet inom ramen för rådsbeslutet och genomförandebeslutet. Eftersom rådsbeslutet inte utgör en utveckling av Schengenregelverket krävs att ett särskilt avtal sluts om tillämpning av rådsbesluten på Norge och Island (se vidare artikel 24 och 38 i Unionsfördraget). Ett utkast till rådsbeslut om undertecknande av ett sådant avtal har förhandlats fram (daterat den 26 januari 2009, 5060/90, i fortsättningen benämnt associationsavtalet).

För svenskt vidkommande kräver associationsavtalet riksdagens godkännande (10 kap. 2 § regeringsformen). Genom 10 kap. 2 § fjärde stycket regeringsformen är det möjligt för regeringen att inhämta riksdagens godkännande av en ännu inte slutförhandlad överenskommelse inom ramen för samarbetet i Europeiska unionen.

[45] Norge och Island associerades till Schengensamarbetet den 19 december 1996. För att förlänga associeringen undertecknades ett avtal mellan Island, Norge och Europeiska unionen den 18 maj 1999 (EGT L 176, 10.7.1999, s. 36).

Associationsavtalet mellan Europeiska unionen samt Norge och Island omfattar artikel 1–24, 25.1, 26–32 och 34 i rådsbeslutet samt artikel 1–19 och 21 i genomförandebeslutet, dvs. i realiteten alla delar av samarbetet. Vidare ska de förklaringar som medlemsstaterna avger i enlighet med rådsbesluten också tillämpas i förhållande till Norge och Island.

I ingressen till associationsavtalet framhålls vikten av att förbättra polissamarbetet och det rättsliga samarbetet mellan Europeiska unionens medlemsstater samt Norge och Island. Dessutom pekas bl.a. på det nära samarbete i kampen mot brottsligheten som redan bedrivs inom ramen för Schengenregelverket.

Norge och Island är som framgått redan integrerade i delar av Europeiska unionens polisiära och rättsliga samarbete. Staterna omfattas också av samarbetet angående internationell rättslig hjälp i brottmål. Även om riksdagen ännu inte har underställts associationsavtalet för godkännande talar mycket för att ett godkännande kommer att aktualiseras inom en snar framtid. Det kan därför vara lämpligt att i detta sammanhang ta hänsyn till Norges och Islands förväntade associering till rådsbeslutet genom att utforma lagstiftningen generellt. Om man redan nu utgår från att Prümrådssamarbetet kan komma att omfatta även stater som inte är medlemmar i Europeiska unionen begränsar man behovet av lagstiftningsändringar om framtida associeringar förverkligas. Eftersom associeringen och tillämpningen av aktuella bestämmelser förutsätter en internationell överenskommelse som riksdagen har godkänt finns det inga nackdelar med en sådan lösning (se även avsnitt 7.7.1).

9 Ekonomiska konsekvenser

Bedömning: De kostnader som förslagen kan ge upphov till kan finansieras inom befintliga anslag.

Skälen för bedömningen: Enligt rådsbeslutet ska de driftskostnader som de nationella myndigheterna ådrar sig i samband med genomförandet och tillämpningen av detta belasta varje medlemsstats budget (artikel 34).

De myndigheter vars verksamhet berörs av det nya informationsutbytet är framför allt Rikspolisstyrelsen och Transportstyrelsen, men också Statens kriminaltekniska laboratorium.

Genomförandet av rådsbeslutet förutsätter inte att några nya register tillskapas, eftersom det redan förs register över de uppgifter som informationsutbytet omfattar. Några kostnader för nya databaser uppstår alltså inte. Däremot torde genomförandet kräva en viss anpassning av registren, för att möjliggöra automatiska sökningar och jämförelser. Det rör sig emellertid om en mindre och väl avgränsad mängd uppgifter som Sverige är skyldig att ge andra medlemsstater tillgång till. Anpassningskostnaderna bör därför bli begränsade. Merparten av kostnaderna kan förväntas uppstå i samband med den initiala tekniska översynen av befintliga system och när registren anpassas till det gränsöverskridande uppgiftsutbyte som rådsbeslutet föreskriver. Dessa kostnader uppstår inte som en direkt följd av de nu aktuella förslagen, eftersom författningsförslagen enbart skapar rättsliga förutsättningar för att kunna genomföra informationsutbytet vid

den senare tidpunkt när den tekniska anpassningen ska vara färdig.

Det är svårt att beräkna hur många sökningar i svenska register som kan bli följden när rådsbeslutet har genomförts i alla delar. Den eventuella ökningen av driftskostnaderna torde emellertid bli mycket begränsad.

Förslagen till författningsändringar berör inte bara det automatiserade informationsutbytet, utan även annat informationsutbyte samt viss praktiskt bistånd vid händelser med gränsöverskridande verkningar.

En generell effekt av rådsbeslutet blir ett ökat antal förfrågningar och kontakter. Dessa kommer att hanteras framför allt av kontaktstället, dvs. Rikspolisstyrelsen. En viss arbetsökning kan bli följden, men samtidigt ersätts en del av dagens mer omständliga hantering i styrelsens uppgift som kontaktyta mellan polismyndigheter och åklagare å ena sidan och Interpol och Europol å den andra av automatiska sökförfaranden. Dessa förändringar bör kunna ta ut varandra.

Mot vissa ökade kostnader ska ställas de fördelar i stort som genomförandet av rådsbeslutet innebär för svensk del. Ett förbättrat informationsutbyte samt enklare och snabbare tillgång till utländska uppgifter om fordon, fingeravtryck och DNA-profiler kommer utan tvekan att effektivisera polisens och andra brottsbekämpande myndigheters arbete.

Vidare måste beaktas att det under de senaste åren har förhandlats flera rättsakter inom Europeiska unionen som rör samarbetet mellan medlemsstaternas brottsbekämpande myndigheter och som bl.a. syftar till att effektivisera brottsbekämpningen genom ökat informationsutbyte. De åtgärder rådsbeslutet kräver kanske i viss utsträckning hade behövt genomföras av andra skäl.

Datainspektionen får i någon utsträckning utökade tillsynsuppgifter, men ökningen är marginell i förhållande till myndighetens nuvarande uppgifter.

När det gäller vägtrafikregistret bör framhållas att lagstiftningen för närvarande är föremål för en översyn som bl.a. omfattar möjligheten att överföra uppgifter och personuppgifter till

utländska aktörer (se avsnitt 6.4.3). I förhållande till den översynen bedöms genomförandet av rådsbeslutet medföra endast marginella förändringar.

Sammantaget bedöms kostnaderna kunna finansieras inom myndigheternas befintliga anslag.

10 Författningskommentar

10.1 Förslaget till lag om ändring i polisdatalagen (1998:622)

1 §

I paragrafen regleras lagens tillämpningsområde och hur den förhåller sig till bl.a. personuppgiftslagen (1998:204). *Första, andra och tredje styckena* är oförändrade.

I *fjärde stycket*, som är nytt, klargörs att det utöver polisdatalagens särskilda reglering i förhållande till personuppgiftslagen kan finnas bestämmelser i lagen (2000:343) om internationellt polisiärt samarbete, och föreskrifter som har meddelats med stöd av den lagen, som grundar sig på Prümrådsbeslutet och som avviker från polisdatalagen. Om det finns sådana avvikande regler, t.ex. om gallring av uppgifter som utbyts med stöd av rådsbeslutet, ska dessa tillämpas i stället för polisdatalagen och personuppgiftslagen.

Den allmänna motiveringen till ändringen finns i avsnitt 7.3.

3 §

I paragrafens *första stycke* definieras sex begrepp som är centrala för lagen. De första fyra är oförändrade.

I den *femte* definitionen, som avser DNA-analys, har ett tillägg gjorts för att tydliggöra att regleringen enbart omfattar DNA-analys av prov från människa. Vid en DNA-analys under-

söks en liten del av arvsmassan i syfte att få fram för individen unika identifikationsuppgifter.

Den *sjätte* begreppet är nytt och definierar DNA-profil, dvs. resultatet av en DNA-analys. En DNA-profil består av uppgifter som har tagits fram med hjälp av DNA-analys, dvs. analys av deoxyribonukleinsyra i antingen ett särskilt prov från humant biologiskt material (t.ex. blod, hår eller saliv) eller från ett spår som påträffats på eller i nära anslutning till en brottsplats. Av regleringen följer att DNA-profilen enbart får presenteras i form av siffror eller bokstäver. Därmed går det inte att identifiera en person enbart med stöd av DNA-profilen. I 24 § regleras vilka uppgifter som får registreras.

Begreppet DNA-profil förekommer i Prümrådsbeslutet och definieras i genomförandebeslutet som ”en bokstav eller en nummerkod som representerar en rad identifikationsuppgifter i den icke-kodifierade delen av ett analyserat mänskligt DNA-prov, dvs. den särskilda molekylära strukturen vid de olika DNA-lokusen”.

Den allmänna motiveringen till den nya definitionen finns i avsnitt 7.6.

Det *andra stycket* är oförändrat.

22 §

Paragrafen reglerar för vilka ändamål DNA-profiler får behandlas och i vilka sammanhang behandlingen får ske.

I *första stycket* har begreppet ”uppgifter om resultatet av DNA-analyser” ersatts med ”DNA-profiler”. Begreppet DNA-profil har kommenterats under 3 §. Ändringen tydliggör att det är DNA-profilen, som inte innehåller någon information om den registrerades personliga egenskaper, som registreras (24 § första stycket). Vidare har i förtydligande syfte de tre DNA-registren benämnts i bestämd form.

Enligt *andra stycket* får, förutom i dessa register, DNA-profiler behandlas även i förundersökningar och särskilda undersökningar. Ett tillägg har gjorts för att klargöra att behandling också

är tillåten om det krävs för att uppfylla en internationell överenskommelse som riksdagen godkänt och som är bindande för Sverige. Syftet med bestämmelsen är att möjliggöra att andra stater, i enlighet med artikel 3 och 4 i Prümrådsbeslutet, får behandla vissa uppgifter i svenska DNA-register som ett led i deras brottsbekämpning. Bestämmelsen ger också stöd för den behandling som krävs när en DNA-profil tas fram på begäran av en annan stat med stöd av 4 kap. 24 a § lagen (2000:562) om internationell rättslig hjälp i brottmål.

I 16 § lagen (2000:343) om internationellt polisiärt samarbete och i förordning regleras under vilka förutsättningar en utländsk myndighet får söka i svenska DNA-register samt hur automatisk sökning i registren och automatisk jämförelse av oidentifierade DNA-profiler ska gå till.

Den allmänna motiveringen till ändringen finns i avsnitt 7.5 och 7.7.

23 §

Paragrafen reglerar innehållet i DNA-registret, vilket består av DNA-profiler från dömda personer. Den ändring som gjorts hör samman med den nya definitionen i 3 § första stycket, där begreppet DNA-profil införs. Genom ändringen tydliggörs att det är DNA-profilen som registreras och utgör det primära innehållet i registret. Benämningen på registret har ändrats i konsekvens med ändringen i 22 §.

24, 24 a och 25 §§

Ändringarna är av samma slag som i 23 §. Vissa språkliga justeringar har också gjorts.

26 §

Paragrafen innehåller bestämmelser om användningen av spårregistret. Det *första stycket* är oförändrat i sak, men vissa konsekvensändringar har gjorts.

Enligt det nya *andra stycket* får DNA-profiler också jämföras med uppgifter i spårregistret om ett bindande internationellt åtagande, i detta fall Prümrådsbeslutet, kräver det. Ändringen föranleds av att andra staters oidentifierade DNA-profiler, i enlighet med artikel 4 i rådsbeslutet, automatiskt ska kunna jämföras också med alla DNA-profiler som finns i det svenska spårregistret. Förutsättningarna för utländska myndigheters automatiska sökningar och automatiska jämförelser i de svenska DNA-registren regleras i 16 § lagen (2000:343) om internationellt polisiärt samarbete och i förordning. Direktåtkomst regleras i 27 b § denna lag.

Den allmänna motiveringen till tillägget finns i avsnitt 7.7.

27 §

Paragrafen reglerar gallring av uppgifter i DNA-registret. I konsekvens med ändringen i 22 § har i *tredje stycket* benämningen på spårregistret ändrats. I övrigt har endast några mindre språkliga justeringar gjorts.

27 a §

Paragrafen reglerar när DNA-prover, som tagits på personer med stöd av bestämmelserna om kroppsbesiktning i 28 kap. rättegångsbalken, ska förstöras.

Första stycket, som anger huvudregeln att proven ska förstöras senast sex månader efter provtagningen, är i sak oförändrat. Det finns givetvis inget som hindrar att proven förstörs dessförinnan. Som framgår av tillägget i första stycket finns det avvikande regler i de tre följande styckena.

I *andra stycket* har förtydligats att DNA-prov från en skäligen misstänkt person ska gallras tidigare än enligt sexmånadersregeln om uppgifterna om personen gallras i utredningsregistret.

I *tredje stycket* har förtydligats att DNA-prov som har tagits från personer som inte är misstänkta för brott också ska förstöras tidigare än vad som anges i första stycket i vissa fall.

Det *fjärde stycket* är nytt. Det reglerar hanteringen av de DNA-prov som tas för en annan stats räkning med stöd av 4 kap. 24 a § lagen (2000:562) om internationell rättslig hjälp i brottmål. Sådana prov ska alltid förstöras senast två månader efter det att de har tagits. Den allmänna motiveringen till tillägget finns i avsnitt 7.8.

27 b §

Paragrafen, som är föranledd av artikel 3 och 4 i Prümrådsbeslutet, är ny. Den hänvisar till den möjlighet som införs i 16 § lagen (2000:343) om internationellt polisiärt samarbete att ge andra stater tillgång till vissa uppgifter i DNA-registret, utredningsregistret och spårregistret med möjlighet att på egen hand söka efter information i dessa (direktåtkomst).

Tillämpningsområdet avgränsas genom bestämmelser i 16 § lagen om internationellt polisiärt samarbete och i förordning.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.7.1.

29 §

Paragrafen reglerar för vilka ändamål uppgifter får behandlas i fingeravtrycks- och signalementsregister och i vilka sammanhang behandlingen får ske. *Första och andra styckena* är oförändrade.

I *tredje stycket* har öppnats en möjlighet att ge en annan stat rätt att behandla fingeravtrycksuppgifter i svenska register om det krävs för att uppfylla ett bindande internationellt åtagande, i detta fall Prümrådsbeslutet. Stycket är föranlett av artikel 8 och 9 i Prümrådsbeslutet. Enligt rådsbeslutet får uppgifterna behandlas

även i syfte att förebygga brott, vilket inte är ett tillåtet ändamål för behandling enligt första stycket. Förutsättningarna för att utländska myndigheter ska få göra sökningar i svenska fingeravtrycksregister regleras i 18 § lagen (2000:343) om internationellt polisiärt samarbete och i förordning. Direktåtkomst regleras i 31 a § denna lag.

Den allmänna motiveringen till ändringen finns i avsnitt 7.9.1.

31 a §

Paragrafen, som är föranledd av artikel 8 och 9 i Prümrådsbeslutet, är ny. Den hänvisar till den möjlighet som finns i 18 § lagen (2000:343) om internationellt polisiärt samarbete att ge andra stater direkt tillgång till vissa uppgifter i svenska fingeravtrycksregister och möjlighet att på egen hand söka efter information (direktåtkomst).

Tillämpningsområdet avgränsas genom bestämmelser i 18 § lagen (2000:343) om internationellt polisiärt samarbete och i förordning.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.9.1.

Övergångsbestämmelserna

Hittills har bestämmelserna i polisdatalagen (1998:622) om fingeravtrycksregister inte tillämpats. Detta beror på att punkten 2 i ikraftträdande- och övergångsbestämmelserna till polisdatalagen medger att de personregister som vid den lagens ikraftträdande fördes med stöd av den numera upphävda datalagen (1973:289) och tillstånd av Datainspektionen får fortsätta att föras under viss tid. Den tiden har förlängts vid flera tillfällen och övergångsreglerna gäller nu till utgången av år 2009. Ändringen i övergångsbestämmelserna innebär att fingeravtrycksregister som förs med Datainspektionens tillstånd från och med ikraftträdandet av ändringarna i polisdatalagen i stället ska omfattas av 29–31 §§ polisdatalagen. Syftet med ändringen är att kunna genomföra

den reglering beträffande fingeravtrycksregister som Prümrådsbeslutet kräver.

Den allmänna motiveringen till ändringen i övergångsbestämmelserna finns i avsnitt 7.9.1.

10.2 Förslaget till lag om ändring i lagen (2000:343) om internationellt polisiärt samarbete

2 §

I paragrafen förklaras vissa grundläggande begrepp som används i lagen. Tre nya definitioner införs.

För det första definieras *Prümrådsbeslutet*, som bl.a. reglerar nya former för utbyte av registeruppgifter mellan medlemsstaterna i syfte att förebygga och bekämpa brott samt upprätthålla allmän ordning och säkerhet.

För det andra definieras begreppet *kontaktställe*. Enligt Prümrådsbeslutet ska varje stat utse kontaktställe för olika typer av informationsutbyte. Rikspolisstyrelsen ska vara kontaktställe för svensk del och förmedla alla typer av uppgifter som behandlas med stöd av Prümrådsbeslutet. Den allmänna motiveringen till denna definition finns i avsnitt 7.13.

För det tredje förklaras begreppet *referensuppgifter*. Begreppet används i flera artiklar i Prümrådsbeslutet. Av integritetsskäl får identiteten på en person inte röjas vid direktåtkomst till uppgifter i DNA-register eller fingeravtrycksregister eller vid automatiska jämförelser med uppgifter i sådana register. I stället får den sökande staten tillgång till vissa referensuppgifter, som inte avslöjar identiteten. Referensuppgifterna får inte heller innehålla någon genetisk information eller påvisa några funktionella egenskaper. Den allmänna motiveringen till denna definition finns i avsnitt 7.7.1.

3 §

Paragrafen reglerar s.k. användningsbegränsande villkor som ställs upp när uppgifter överlämnas till en svensk myndighet. Liksom tidigare innebär bestämmelsen att svenska myndigheter är skyldiga att följa sådana villkor som ställts upp för användningen. Villkoren gäller inte bara för den myndighet som tog emot informationen, utan även för alla andra svenska myndigheter som senare får tillgång till denna (se prop. 1990/91:131 s. 23 och JO 2007/08 s. 57). En användningsbegränsning som ålagts en mottagande svensk myndighet med stöd av bestämmelsen hindrar dock inte att tillsynsorgan som JO, JK, Datainspektionen eller Säkerhets- och integritetsskyddsnämnden tar del av och använder informationen i sin tillsyn och inte heller att rättsliga myndigheter gör detta som ett led i en motsvarande rättslig prövning som har stöd i lag.

Hittills har användningsbegränsningar endast gällt när materialet har överlämnats för underrättelseverksamhet om brott och utredning av brott. Genom ändringarna kommer användningsbegränsande villkor också att gälla för uppgifter som med stöd av Prümrådsbeslutet har översänts i syfte att upprätthålla allmän ordning och säkerhet. Bestämmelsen kan aktualiseras bl.a. i samband med översändande av personuppgifter inför större evenemang med gränsöverskridande verkningar (artikel 14 i Prümrådsbeslutet).

Bestämmelsen har vidare ändrats så att det tydligare framgår i vilka fall bindande användningsbegränsningar kan förekomma. Dessa anges i två punkter, vilka är oförändrade i sak. Redan tidigare har paragrafen ansetts vara tillämplig på uppgifter som härrör från Europol. Användningsbegränsningar kan också gälla för information som erhålls från andra EU-institutioner.

Genom formuleringen ”gjorts tillgängligt av” klargörs vidare att om det ställs villkor för användningen av uppgifter som är åtkomliga genom direktåtkomst gäller villkoren på samma sätt som andra användningsbegränsningar.

I bestämmelsen har också en mindre språklig ändring gjorts.

Det *andra stycket* har upphävts. Motsvarande bestämmelse finns i punkten 2.

Den allmänna motiveringen till ändringarna i paragrafen finns i avsnitt 7.17.4.

3 a §

Paragrafen, som är ny, är en spegling av 3 §. Den reglerar möjligheten att ställa upp användningsbegränsande villkor när en svensk brottsbekämpande myndighet lämnar upplysningar eller bevismaterial till en annan stat eller en mellanfolklig organisation. Kategorin av mottagare är densamma som kan ställa bindande villkor gentemot svenska myndigheter enligt 3 §.

En förutsättning för att en svensk brottsbekämpande myndighet ska få ställa upp användningsbegränsande villkor är att detta krävs med hänsyn till enskilds rätt eller från allmän synpunkt. Villkoren får inte heller strida mot våra internationella åtaganden. Bestämmelsen är avsedd att tillämpas restriktivt. Sådana villkor som ställs upp ska vara nödvändiga. Ett exempel på när villkor kan krävas är om det samtidigt pågår brottsutredning eller underrättelsearbete i Sverige som riskerar att skadas om informationen används före en viss tidpunkt.

Paragrafen motsvarar i sak 5 kap. 2 § lagen (2000:562) om internationell rättslig hjälp i brottmål och 2 kap. 7 § lagen (2000:1219) om internationellt tullsamarbete. Den nu aktuella paragrafen omfattar även uppgifter som görs tillgängliga genom direktåtkomst till vissa register, vilket framgår av formuleringen ”gjorts tillgängligt för”. Paragrafen kan, förutom vid informationsutbyte med stöd av Prümrådsbeslutet, bl.a. vara tillämplig på information eller underrättelser som tillhandahålls en brottsbekämpande myndighet i en annan medlemsstat i Europeiska unionen med stöd av rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater, det s.k. svenska initiativet (6 § förord-

ningen [2008:1396] om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen).

Eventuella villkor måste ställas upp när uppgifterna sänds över eller när direktåtkomsten beviljas. Det går således inte att ställa upp villkor i efterhand.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.17.4.

11, 12 och 13 §§

Ändringarna sammanhänger med att lagen nu blir tillämplig även på samarbete med stöd av Prümrådsbeslutet. Paragraferna har därför ändrats för att avgränsa regleringen beträffande utländska tjänstemän som utför uppgifter enligt Schengensamarbetet och samarbetet inom Öresundsregionen. Den generella hänvisningen till ”denna lag” har ersatts av hänvisningar till de paragrafer som är tillämpliga på det nämnda samarbetet. Mindre språkliga justeringar har också gjorts.

16 §

Paragrafen är ny. Den reglerar andra staters tillgång till vissa uppgifter i de svenska DNA-registren och genomför i huvudsak artikel 3 och 4 i Prümrådsbeslutet.

Enligt *första stycket* får ett kontaktställe i en annan stat, i enlighet med artikel 3.1 i Prümrådsbeslutet, ges direkt tillgång till och rätt att på egen hand söka efter referensuppgifter i de svenska DNA-registren, dvs. DNA-registret, spårregistret och utredningsregistret (direktåtkomst). Bestämmelser om DNA-registren finns i 22–27 §§ polisdatalagen (1998:622). Begreppet kontaktställe definieras i 2 §. Vad som avses med referensuppgifter anges i 2 § och avgränsas närmare genom bestämmelser i förordning.

Tillgång genom direktåtkomst ska endast ges till referensuppgifter. Ytterst begränsas åtkomsten till vad som gäller för motsvarande sökning i en svensk brottsutredning. Direktåtkomsten

till vissa uppgifter innebär att den andra staten inom närmare angivna ramar själv kan ta del av uppgifterna vid ett visst tillfälle, utan att det svenska kontaktstället först fattar beslut om att just dessa uppgifter ska lämnas ut. Direktåtkomsten medför att uppgifterna är att betrakta som utlämnade. Någon sekretessprövning aktualiseras därför inte.

De närmare bestämmelserna om vad som gäller när en sökning i de svenska registren resulterar i överensstämmelse mellan en översänd DNA-profil och en DNA-profil i ett svenskt register regleras i förordning. Detsamma gäller förfarandet när ingen överensstämmelse konstateras.

Enligt *andra stycket* begränsas möjligheterna att behandla uppgifter i de svenska DNA-registren till ”ett enskilt fall”. Behandlingen får vidare enbart ske i samband med brottsutredning. Med ”ett enskilt fall” avses att behandlingen ska omfatta endast en utrednings- eller lagföringsfil. Om en sådan fil innehåller mer än en DNA-profil ska profilerna hanteras tillsammans (artikel 2 k i genomförandebeslutet). Vilka krav som ställs för att det ska anses vara ”i samband med brottsutredning” avgörs av den andra statens lagstiftning. En ytterligare begränsning ligger i att det utländska kontaktställets behandling av uppgifter i de svenska registren aldrig kan sträcka sig längre än till vad som är tillåtet för en svensk myndighet i motsvarande situation.

Andra stycket genomför också delar av artikel 4 i Prümrådsbeslutet och reglerar andra staters behandling av DNA-profiler genom automatiska jämförelser i de svenska DNA-registren efter särskild överenskommelse (enligt den engelska texten ”by mutual consent”). I fråga om begreppen DNA-profil, referensuppgifter och kontaktställe hänvisas till kommentaren till första stycket.

Bestämmelsen ger ett kontaktställe i en annan stat rätt att efter en särskild överenskommelse automatiskt jämföra den statens samtliga oidentifierade DNA-profiler (s.k. öppna spår) med uppgifter i samtliga svenska DNA-register, dvs. även uppgifter avseende identifierade personprofiler. Med oidentifierade DNA-profiler avses DNA-profiler som härrör från spår som har sam-

lats in under en brottsutredning och som tillhör en person som ännu inte har identifierats (artikel 2 g i genomförandebeslutet). Automatiska jämförelser får endast ske ”i samband med brottsutredning”. Vilka krav som ställs för att det ska anses vara ”i samband med brottsutredning” avgörs av den andra statens lagstiftning. Direktåtkomsten får inte ges vidare omfattning än vad som gäller för motsvarande behandling i en svensk brottsutredning. Vidare får behandling bara utföras av vissa särskilt utpekade personer.

Även om det visar sig att det föreligger en överensstämmelse med en svensk DNA-profil avgör den ansökande staten om man vill gå vidare och begära uppgift om identiteten på den person som DNA-profilen tillhör (artikel 5 i Prümrådsbeslutet). I det fortsatta förfarandet tillämpas bestämmelserna om rättslig hjälp, dvs. för svensk del lagen (2000:562) om internationell rättslig hjälp i brottmål. Om någon överenskommelse inte konstateras underrättas den andra statens kontaktställe automatiskt.

Enligt *tredje stycket* får Rikspolisstyrelsen ingå en sådan överenskommelse som avses i andra stycket.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.7.1.

17 §

Paragrafen, som är ny, reglerar möjligheten för det svenska kontaktstället att genom dess tjänstemän göra sökningar i andra staters DNA-register i enlighet med artikel 3 och 4 i Prümrådsbeslutet.

Enligt *första stycket* får sökningar endast göras i ett enskilt fall och som ett led i en förundersökning eller annan utredning som görs med stöd av bestämmelserna om förundersökning i brottmål. Ett exempel på det sistnämnda är utredning angående utlämning för brott. Vad som avses med ”ett enskilt fall” kommenteras under 16 §. Sökningar får vidare endast göras för de ändamål och med de begränsningar som anges i polisdatalagen för motsvarande sökningar i svenska register. Det innebär exem-

pelvis att DNA-profiler som härrör från personer som inte är misstänkta för brott inte får användas för generella sökningar. Möjligheterna att söka efter information begränsas vidare av den andra statens lagstiftning. Det är därför inte givet att en sökning som hade kunnat göras i svenska register är tillåten.

Vem som får göra sökningar i utländska DNA-register och hur detta ska ske regleras i förordning.

I *andra stycket* regleras automatiska jämförelser mellan DNA-profiler i spårregistret, dvs. oidentifierade svenska DNA-profiler, och DNA-profiler i andra staters DNA-register. Sådana automatiska jämförelser förutsätter att överenskommelse har träffats med den andra staten.

Enligt *tredje stycket* får Rikspolisstyrelsen ingå en sådan överenskommelse som avses i andra stycket.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.11.

18 §

Paragrafen är ny och genomför artikel 8 och 9 i Prümrådsbeslutet. Den reglerar andra staters tillgång till vissa uppgifter i svenska fingeravtrycksregister. Bestämmelser om fingeravtrycksregister finns i 29–31 §§ polisdatalagen (1998:622). Med fingeravtryck jämställs handavtryck.

Enligt paragrafen får ett kontaktställe i en annan stat ges direkt tillgång till och rätt att på egen hand söka efter referensuppgifter i svenska fingeravtrycksregister (direktåtkomst). Vad som avses med kontaktställe och referensuppgifter kommenteras under 2 §.

Möjligheterna att behandla uppgifter i svenska fingeravtrycksregister begränsas till enskilda fall och ska i övrigt ske i enlighet med den andra statens reglering. En sökning kan avse såväl identifierade som oidentifierade fingeravtryck. Med ett ”enskilt fall” avses en utrednings- eller lagföringsfil. Om denna innehåller flera fingeravtrycksuppgifter ska dessa hanteras tillsammans (artikel 2 k i genomförandebeslutet). Behandlingen får inte bara ske i samband med utredning av brott utan även för att

förebygga brott (jfr 17 §, som inte medger sökning för det sistnämnda ändamålet).

Om fingeravtrycksuppgifterna av kvalitetsskäl inte lämpar sig för en automatisk jämförelse, ska det svenska kontaktstället omedelbart underrätta den andra staten om detta (artikel 14 i genomförandebeslutet).

Den andra statens sökning ska besvaras automatiskt. Förekommer fingeravtrycket ska kontaktstället i den andra staten automatiskt få del av fingeravtrycksuppgifterna och en sifferbeteckning. Syftet med detta är att den andra staten ska kunna konstatera att det finns en faktisk överensstämmelse. Däremot röjs inga uppgifter om vem fingeravtrycket tillhör. Vid överensstämmelse avgör den andra staten om man ska begära ytterligare information. I det fortsatta förfarandet tillämpas bestämmelserna om rättslig hjälp, dvs. för svensk del lagen (2000:562) om internationell rättslig hjälp i brottmål. Om någon överensstämmelse inte konstateras, underrättas den andra statens kontaktställe automatiskt om detta.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.9.1.

19 §

Paragrafen, som är ny, reglerar möjligheten för det svenska kontaktstället att med stöd av artikel 8 och 9 i Prümrådsbeslutet göra sökningar i andra staters fingeravtrycksregister. Sökningar får endast göras för de ändamål och med de begränsningar som anges i polisdatalagen för motsvarande sökningar i svenska register. Möjligheten att göra sökningar i syfte att förebygga brott förutsätter därför att behandlingen görs inom ramen för en förundersökning eller en särskild undersökning. Vidare begränsas möjligheterna att söka efter information av den andra statens lagstiftning. Det är därför inte givet att en sökning som hade kunnat göras i svenska register är tillåten. Vem som får göra sökningar i utländska fingeravtrycksregister och hur detta ska ske regleras i förordning.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.11.

20 §

Paragrafen, som är ny, innehåller upplysning om att det finns kompletterande regler om samarbetet med stöd av Prümrådsbeslutet i förordning.

10.3 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

4 kap.

24 a §

Paragrafen, som genomför artikel 7 i Prümrådsbeslutet, är ny. Skyldigheten enligt Prümrådsbeslutet sträcker sig längre än rättslig hjälp med kroppsbesiktning i syfte att ta DNA-prov. Den omfattar även analysen av provet, dvs. framtagandet av en DNA-profil.

I *första stycket* regleras internationell rättslig hjälp med att ta fram DNA-profiler för personer som vistas i Sverige. En förutsättning för att rättslig hjälp ska lämnas är att det inte finns någon DNA-profil för personen. Begreppet DNA-profil definieras i 3 § polisdatalagen (1998:622). För att bestämmelsen ska vara tillämplig krävs vidare att en brottsutredning eller ett annat straffrättsligt förfarande pågår. Provtagning i syfte att, med utgångspunkt i analysresultatet, påbörja ett rättsligt förfarande faller därför utanför. Likaså provtagning i verkställighetssyfte.

Den ansökande staten ska ange för vilket ändamål DNA-profilen behövs och huruvida det hade funnits förutsättningar att samla in och analysera DNA-prov om personen i fråga hade vistats i den ansökande staten. Det torde innebära att en ansökan

om rättslig hjälp kan komma att avse såväl misstänkta som andra personer, beroende på den ansökande statens lagstiftning.

Det generella kravet på dubbel straffbarhet i 2 kap. 2 § gäller för tagande av DNA-prov. Det måste också finnas rättsliga förutsättningar att med stöd av svensk rätt vidta åtgärden. Det innebär bl.a. att de begränsningar som gäller enligt 28 kap. 12–13 §§ rättegångsbalken ska iakttas. Om svensk rätt inte medger att DNA-prov tas, exempelvis om begäran avser en misstänkt som är under 15 år eller om prov inte kan tas på grund av att brottet inte är tillräckligt allvarligt, ska begäran om rättslig hjälp avslås.

Den rättsliga hjälpen handläggs av åklagare (4 kap. 18 §). I fråga om åklagarens möjligheter att begära biträde av polisen gäller samma regler som vid en svensk förundersökning.

Förfarandet vid DNA-analysen är detsamma som vid en svensk förundersökning. Ett DNA-prov som har tagits med stöd av denna paragraf får enligt 28 § polisdatalagen (1998:622) inte användas för något annat ändamål, vilket innebär att DNA-profilen inte får registreras i svenska DNA-register. I 27 a § fjärde stycket polisdatalagen regleras förstöring av sådana prov.

Enligt a*ndra stycket* får DNA-profiler enbart översändas i en form som gör att berörda personer inte kan identifieras med stöd av dessa. Syftet med bestämmelsen är att skapa det integritetsskydd som rådsbeslutet kräver och som innebär att enbart anonyma uppgifter ska översändas. Sådana uppgifter kan t.ex. även omfatta kurvor från en analys, om detta krävs för att mottagaren ska kunna verifiera ett analysresultat. Däremot får personuppgifter, som t.ex. namn eller födelsetid, inte översändas med stöd av denna paragraf utan enbart med stöd av andra regler om rättslig hjälp.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.8.

24 b §

Paragrafen, som är ny, reglerar en svensk begäran om rättslig hjälp med framtagande av DNA-profil från någon som vistas i en annan stat. Paragrafen är en spegling av 24 a §.

Även i en svensk brottsutredning eller annat straffrättsligt förfarande kan det uppkomma behov av att få fram en DNA-profil från någon som visats i en annan stat. En DNA-profil kan t.ex. vara avgörande för om en person ska begäras överlämnad till Sverige och kan i andra fall bidra till att fria en person från misstankar. En grundläggande förutsättning för att en svensk åklagare ska kunna begära rättslig hjälp med stöd av denna bestämmelse är att det inte finns någon DNA-profil på personen i fråga. Vidare ska det pågå en förundersökning eller annan brottsutredning. Dessutom ska kraven i 28 kap. rättegångsbalken för att ta DNA-prov vara uppfyllda.

En ansökan om rättslig hjälp ska innehålla uppgifter om för vilket ändamål DNA-profilen behövs. Vidare ska det av ansökan framgå att det hade funnits förutsättningar att samla in och analysera DNA-prov om personen i fråga hade vistats i Sverige.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.8.

10.4 Förslaget till lag om ändring i lagen (2001:558) om vägtrafikregister

2 §

Paragrafen reglerar lagens förhållande till personuppgiftslagen (1998:204) och anger att personuppgiftslagen som huvudregel gäller, men att det kan finnas avvikande reglering.

Första stycket har ändrats till följd av att det kan finnas avvikande bestämmelser också i föreskrifter som genomför detaljbestämmelserna i Prümrådsbeslutet. Om det finns avvikande regler t.ex. om gallring av sådana uppgifter som utbyts med stöd av

rådsbeslutet, ska dessa tillämpas i stället för reglerna i personuppgiftslagen och trafikregisterlagstiftningen.

Det *andra stycket* är oförändrat.

Den allmänna motiveringen till ändringen finns i avsnitt 7.3.

5 §

Paragrafen reglerar för vilka ändamål uppgifter får behandlas i vägtrafikregistret. Personuppgifter får inte behandlas för andra ändamål än de som uttryckligen anges i bestämmelsen.

Punkten 6 är ny och utvidgar ändamålen för behandling av uppgifter i registret. Tillägget är föranlett av skyldigheten enligt artikel 12 i Prümrådsbeslutet att medge andra stater direktåtkomst till vissa personuppgifter som rör fordon och deras ägare eller innehavare.

Ändringen innebär också att behandling av uppgifter för sådana ändamål som avses i punkten 6 omfattas av den bestämmelse om direktåtkomst som finns i förordningen (2001:650) om vägtrafikregister (se 4 kap. 3–5 §§ och däri gjord hänvisning till 8 § lagen om vägtrafikregister).

I övrigt har endast en redaktionell ändring gjorts.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.10.

8 §

I paragrafen, som reglerar direktåtkomst till personuppgifter i vägtrafikregistret, har en följdändring gjorts till ändringen i 5 §, beroende på att en ny punkt har införts i den paragrafen. Ändamålsbestämmelserna i 5 § styr möjligheterna till direktåtkomst. Genom ändringen kommer Prümrådsbeslutets bestämmelser om tillhandahållande av uppgifter till andra stater att kunna förverkligas genom att dessa kan beviljas direktåtkomst.

Den allmänna motiveringen till paragrafen finns i avsnitt 7.10.

Uppdraget

REGERINGSKANSLIET

Promemoria § 348

Justitiedepartementet 2008-07-09 Ju2008/5996/P

Genomförande av Informationsrambeslutet och de huvudsakliga delarna av Prümrådsbeslutet

Informationsrambeslutet

I juni 2004 presenterades på svenskt initiativ vid rådet för rättsliga och inrikes frågor (RIF-rådet) ett förslag till rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna inom EU. Förslaget förhandlades under 2004 och 2005 och i december 2006 antogs rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater, ”Informationsrambeslutet”.

Utgångspunkten i rambeslutet är att brottsbekämpande myndigheter måste kunna begära och få information och underrättelser från andra medlemsstater under olika faser av en utredning, alltifrån insamlandet av kriminalunderrättelser till brottsutredningen. Beslutets syfte är därför att säkerställa att viss information av avgörande betydelse för brottsbekämpande myndigheter snabbt kan utbytas inom unionen. Informationsrambeslutet ska vara genomfört senast den 19 december 2008.

Beslutet innehåller bestämmelser om att viss information och vissa underrättelser, under förutsättningar som närmare anges i beslutet, på begäran ska tillhandahållas en brottsbekämpande

myndighet som genomför en brottsutredning eller bedriver kriminalunderrättelseverksamhet. Under vissa förutsättningar ska information och underrättelser lämnas även utan anmodan. Bestämmelser finns även om bl.a. tidsfrister för tillhandahållandet, vilka kanaler som ska användas för utbytet, dataskydd för uppgifter som utbyts, sekretess samt vägransgrunder.

Behovet av en utredning

Inom Justitiedepartementet har preliminärt gjorts bedömningen att beslutets genomförande i svensk rätt ställer krav på vissa förordningsändringar.

En utredare bör nu få i uppdrag att biträda departementet med att närmare se över behovet av och föreslå de förordningsändringar som bedöms vara nödvändiga och lämpliga med anledning av rambeslutets bestämmelser.

Prümrådsbeslutet

I maj 2005 träffade sju av EU:s medlemsstater en överenskommelse i den tyska staden Prüm, den s.k. Prümkonventionen. Konventionsstaternas uttalade målsättning var att utveckla informationsutbytet inom hela EU, framför allt vad gäller DNA-, fingeravtrycks- och fordonsuppgifter.

Vid RIF-rådet den 15 februari 2007 nåddes en politisk principöverenskommelse om att integrera merparten av Prümkonventionens tredjepelarfrågor i EU:s regelverk. Ordförandeskapet presenterade därefter ett förslag till rådsbeslut, rådets beslut om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet, ”Prümrådsbeslutet”. Vid RIF-rådets möte den 12-13 juni 2007 träffades en politisk överenskommelse om innehållet i beslutet. Sverige lämnade i samband med det en parlamentarisk granskningsreservation.

I propositionen Godkännande av Prümrådsbeslutet (prop. 2007/08:83) har regeringen föreslagit att riksdagen ska godkänna utkastet till rådsbeslut. Regeringen har i propositionen också redogjort för innehållet i utkastet till rådsbeslut samt, på ett allmänt plan, övervägt vilka lagändringar som kan bli nödvändiga med anledning av beslutet. Några förslag till lagändringar har dock inte lämnats i propositionen. Riksdagen har godkänt utkastet till rådsbeslut (bet. 2007/08:JuU20, rskr. 2007/08:197), varefter Sverige har lyft sin parlamentariska granskningsreservation.

Beslutet, tillsammans med ett rådsbeslut om genomförande av dess bestämmelser, har därefter antagits av rådet den 23-24 juni 2008.

Rådsbeslutet innehåller bestämmelser som syftar till att utveckla informationsutbytet inom unionen, framförallt vad gäller uppgifter i DNA-, fingeravtrycks- och fordonsregister. Bestämmelser finns även om samarbete för förebyggande av terroristbrott samt andra former av samarbete, främst gemensamma insatser inom unionen och bistånd vid större evenemang, katastrofer och allvarliga olyckor. Därutöver innehåller beslutet dataskyddsbestämmelser.

Behovet av en utredning

Prümrådsbeslutet kan antas av rådet tidigast under sommaren 2008, efter att samtliga länder har lyft sina parlamentariska reservationer mot beslutet. Därefter ska beslutet vara genomfört inom ett år, med undantag för bestämmelserna i kapitel 2 om direktåtkomst till DNA-, fingeravtryck- och fordonsuppgifter, där tre års genomförandetid har föreskrivits. Vid den översiktliga analys av behovet av författningsändringar som gjorts i propositionen har gjorts bedömningen att rådsbeslutet, i de delar det är tvingande, ställer krav på vissa författningsändringar.

En utredare bör nu få i uppdrag att biträda departementet med att se över behovet av och föreslå de författningsändringar

som bedöms vara nödvändiga och lämpliga med anledning av rådsbeslutets tvingande bestämmelser. Utredningen bör göras med utgångspunkt i den analys som gjorts i propositionen Godkännande av Prümrådsbeslutet.

Detta gäller bestämmelserna i rådsbeslutets kapitel 2, 3 och 6. Bestämmelsen i kap. 4, (artikel 16) om översändande av uppgifter för förebyggande av terroristbrott, är visserligen utformad som en fakultativ bestämmelse. Eftersom bestämmelsen gäller översändande av uppgifter som i stor utsträckning utbyts redan idag, men där artikeln nu ställer upp bl.a. en skyldighet att utse ett nationellt kontaktställe och möjlighet att uppställa villkor om användningsbegränsning för översända uppgifter, bör uppdraget omfatta även genomförande av den artikeln.

I rådsbeslutets kap. 5 förekommer såväl frivilliga bestämmelser om gemensamma insatser (artikel 17) som tvingande bestämmelser om bistånd till andra medlemsstater (artikel 18). I kapitlet regleras även frågor om vapenanvändning, straffansvar, skadestånd m.m. (artiklarna 19-23). Dessa bestämmelser är tvingande i den mån de aktualiseras genom mottagande eller översändande av tjänstemän. Bestämmelserna i kapitlet i den del de innebär att utländska tjänstemän ska få tjänstgöra på svenskt territorium, vara beväpnade och eventuellt förses med befogenheter att utöva myndighet bör lämpligen utredas särskilt. I den nu aktuella utredarens uppdrag bör däremot ingå att genomföra den del av artikel 18 som är tvingande, nämligen skyldigheten för svenska myndigheter att under vissa förutsättningar lämna bistånd till andra medlemsstater och de eventuella följder som bestämmelserna i artiklarna 19-23 kan få i detta avseende.

Uppdraget

Utredaren ska se över behovet av och föreslå de förordningsändringar som bedöms vara nödvändiga och lämpliga för att genomföra Informationsrambeslutet.

Uppdraget ska i denna del redovisas senast den 1 oktober 2008.

Utredaren ska vidare, med utgångspunkt i den analys som gjorts i propositionen Godkännande av Prümrådsbeslutet, se över behovet av och föreslå de författningsändringar som bedöms vara nödvändiga och lämpliga för att genomföra detta rådsbeslut i de delar som har angivits ovan. Utredaren ska därvid också beakta bestämmelserna i rådsbeslutet om genomförande av Prümrådsbeslutet.

Uppdraget ska i denna del redovisas senast den 1 mars 2009.

Utredaren ska i uppdragets båda delar analysera och redovisa vilka ekonomiska konsekvenser förslagen kan komma att medföra och föreslå hur kostnaderna ska finansieras.

Under genomförandet av uppdraget ska utredaren samråda med de brottsbekämpande myndigheterna. Utredaren ska även samråda med andra myndigheter i den utsträckning utredaren finner lämpligt. Utredaren ska även samråda med den utredare som har i uppdrag att se över vägtrafikregisterlagstiftningen (dir 2008:53).

Utredaren är fri att föreslå de ytterligare författningsändringar, som i anslutning till uppdraget befinns lämpliga.

RÅDETS BESLUT 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet

6.8.2008 SV Europeiska unionens officiella tidning L 210/1

III

(Rättsakter som antagits i enlighet med fördraget om Europeiska unionen)

RÄTTSAKTER SOM ANTAGITS I ENLIGHET MED AVDELNING VI I FÖRDRAGET OM EUROPEISKA UNIONEN

RÅDETS BESLUT 2008/615/RIF

av den 23 juni 2008

om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet

EUROPEISKA UNIONENS RÅD HAR BESLUTAT FÖLJANDE

med beaktande av fördraget om Europeiska unionen, särskilt artikel 30.1 a och b, artikel 31.1 a, artikel 32 och artikel 34.2 c,

på initiativ av Konungariket Belgien, Republiken Bulgarien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Republiken Italien, Storhertigdömet Luxemburg, Konungariket Nederländerna, Republiken Österrike, Republiken Portugal, Rumänien, Republiken Slovenien, Republiken Slovakien, Republiken Finland och Konungariket Sverige,

med beaktande av Europaparlamentets yttrande [1], och

av följande skäl:

(1) Efter ikraftträdandet av fördraget mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration (Prümfördraget) läggs, i enlighet med bestämmelserna i fördraget om Europeiska unionen efter samråd med Europeiska kommissionen, detta initiativ fram i syfte att införliva innebörden av bestämmelserna i Prümfördraget med Europeiska unionens lagstiftning.

(2) I slutsatserna från Europeiska rådets möte i Tammerfors i oktober 1999 bekräftades behovet av förbättrat informationsutbyte mellan medlemsstaternas behöriga myndigheter för att upptäcka och utreda brott.

(3) I Haagprogrammet för stärkt frihet, säkerhet och rättvisa i Europeiska unionen från november 2004 ger Europeiska rådet uttryck för sin övertygelse om att det för detta syfte krävs en innovativ strategi i fråga om gränsöverskridande utbyte av information om brottsbekämpning.

(4) Europeiska rådet angav i enlighet med detta att utbytet av sådan information bör uppfylla de villkor som gäller för tillgänglighetsprincipen. Detta innebär att en brottsbekämpande tjänsteman i en av unionens medlemsstater som behöver information för att utföra sina uppgifter kan få denna från en annan medlemsstat och att de brottsbekämpande myndigheterna i den medlemsstat som innehar denna information kommer att göra den tillgänglig för det angivna ändamålet, med hänsyn tagen till behov med anknytning till pågående utredningar i den medlemsstaten.

(5) Europeiska rådet fastställde den 1 januari 2008 som tidsfrist för att uppnå detta mål i Haagprogrammet.

(6) Redan i rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater [2] fastställs regler enligt vilka medlemsstaternas brottsbekämpande myndigheter effektivt och snabbt kan utbyta befintlig information och befintliga underrättelser för genomförandet av brottsutredningar eller kriminalunderrättelseverksamhet.

(7) I Haagprogrammet för stärkt frihet, säkerhet och rättvisa förklaras också att ny teknik bör användas fullt ut och att det också bör finnas ömsesidig tillgång till nationella databaser, men att nya centraliserade europeiska databaser bör inrättas endast på grundval av studier som har visat deras mervärde.

[1] Yttrandet avgivet den 10 juni 2007 (ännu ej offentliggjort i EUT).

[2] EUT L 386, 29.12.2006, s. 89.

(8) För ett effektivt internationellt samarbete är det av central betydelse att exakt information kan utbytas snabbt och effektivt. Syftet är att införa förfaranden för att främja ett snabbt, effektivt och billigt utbyte av uppgifter. För den gemensamma användningen av uppgifter bör ansvarsskyldighet gälla för dessa förfaranden, och de bör innehålla lämpliga garantier beträffande uppgifternas korrekthet och säkerhet under överföring och lagring samt förfaranden för registrering av utbyte av uppgifter och restriktioner beträffande användningen av utbytta uppgifter.

(9) Dessa krav uppfylls genom Prümfördraget. För att de väsentliga kraven i Haagprogrammet ska kunna uppfyllas för samtliga medlemsstater inom den tidsram som fastställs där bör innebörden av de väsentliga delarna av Prümfördraget göras tillämpliga på samtliga medlemsstater.

(10) Detta beslut innehåller därför bestämmelser som är grundade på de viktigaste bestämmelserna i Prümfördraget och som är avsedda att förbättra informationsutbytet, varigenom medlemsstaterna beviljar varandra rätt till tillgång till sina automatiska databaser över DNA-analyser, automatiska identifieringssystem för fingeravtryck och uppgifter i fordonsregister. När det gäller uppgifter från nationella databaser över DNA-analyser och automatiska identifieringssystem för fingeravtryck bör det genom ett system med träff/icke träff vara möjligt för den medlemsstat som genomför sökningen att i ett andra steg begära specifika personuppgifter från den medlemsstat som administrerar uppgifterna och vid behov begära ytterligare uppgifter genom förfaranden för ömsesidigt bistånd, inklusive de förfaranden som har antagits enligt rambeslut 2006/960/RIF.

(11) Detta skulle påskynda de befintliga förfarandena avsevärt genom att det blir möjligt för medlemsstaterna att ta reda på om någon annan medlemsstat, och i så fall vilken, har de uppgifter som de behöver.

(12) Gränsöverskridande jämförelse av uppgifter bör öppna en ny dimension inom brottsbekämpningen. Den information som erhålls genom jämförelse av uppgifter bör öppna vägen för nya utredningsstrategier för medlemsstaterna och alltså spela en central roll när det gäller att bistå medlemsstaternas brottsbekämpande och rättsliga myndigheter.

(13) Reglerna bygger på inrättande av nätverk mellan medlemsstaternas nationella databaser.

(14) På vissa villkor bör medlemsstaterna kunna översända personuppgifter och icke-personuppgifter för att förbättra informationsutbytet för att förebygga brott och upprätthålla den allmänna ordningen och säkerheten i samband med större evenemang med gränsöverskridande verkningar.

(15) Vid tillämpningen av artikel 12 får medlemsstaterna besluta att prioritera kampen mot allvarlig brottslighet med beaktande av de begränsade tekniska resurser som finns tillgängliga för överföringen av uppgifter.

(16) Förutom förbättring av informationsutbytet finns det behov av en reglering av andra former för närmare samarbete mellan polismyndigheterna, särskilt vid gemensamma säkerhetsoperationer (t.ex. gemensamma patruller).

(17) Närmare polissamarbete och straffrättsligt samarbete måste gå hand i hand med respekt för grundläggande rättigheter, särskilt rätten till respekt för integritet och till skydd av personuppgifter, som bör garanteras genom särskilda förfaranden för uppgiftsskydd som är särskilt anpassade till den specifika arten av olika former av uppgiftsutbyte. Sådana bestämmelser om uppgiftsskydd bör särskilt beakta särdragen i gränsöverskridande elektronisk åtkomst till databaser. Eftersom det med åtkomst on-line inte är möjligt för den medlemsstat som administrerar uppgifterna att göra kontroller i förväg bör ett system för kontroll i efterhand finnas.

(18) Systemet med träff/icke-träff tillhandahåller en struktur med jämförelse av anonyma profiler, där ytterligare personuppgifter endast utbyts efter en träff, för vilket tillgången och mottagandet styrs av nationell lagstiftning, inbegripet regler om rättsligt bistånd. Denna konstruktion garanterar systemet med träff/icke-träff tillfredsställande skydd av personuppgifter, varvid dock översändandet av personuppgifter till en annan medlemsstat förutsätter tillräcklig dataskyddsnivå i den mottagande medlemsstaten.

(19) Med tanke på det omfattande utbyte av information och uppgifter som följer av närmare polisiärt och rättsligt samarbete eftersträvar man med detta beslut att garantera en lämplig nivå av uppgiftsskydd. Det följer den skyddsnivå som utformats för databehandling i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter, tilläggsprotokollet till konventionen av den 8 november 2001 och principerna i Europarådets rekommendation nr R (87) 15 om polisens användning av personuppgifter.

(20) Bestämmelserna om dataskydd i detta beslut inbegriper även de dataskyddsprinciper som var nödvändiga på grund av avsaknaden av ett rambeslut om dataskydd i den tredje pelaren. Detta rambeslut bör tillämpas inom hela området för polissamarbete och straffrättsligt samarbete under förutsättning att dess dataskyddsnivå inte är lägre än det skydd som fastställs i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter och i dess tilläggsprotokoll av den 8 november 2001 samt att Europarådets ministerkommittés rekommendation R (87) 15 av den 17 september 1987 om polisens användning av personuppgifter beaktas, även när uppgifter inte behandlas automatiskt.

(21) Eftersom målen för detta beslut, särskilt förbättrandet av informationsutbytet i Europeiska unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna själva på grund av brottsbekämpningens och säkerhetsfrågornas gränsöverskridande natur, vilket innebär att medlemsstaterna är ömsesidigt beroende av varandra i dessa frågor, och de därför bättre kan uppnås på EU-nivå, kan rådet vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om upprättandet av Europeiska gemenskapen, till vilken artikel 2 i fördraget om Europeiska unionen hänvisar. I enlighet med proportionalitetsprincipen i artikel 5 i EG-fördraget går detta beslut inte utöver vad som är nödvändigt för att uppnå dessa mål.

(22) Detta beslut står i överensstämmelse med de grundläggande rättigheter och principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA ASPEKTER

Artikel 1

Syfte och tillämpningsområde

Genom detta beslut har medlemsstaterna för avsikt att fördjupa det gränsöverskridande samarbetet i frågor som omfattas av avdelning VI i fördraget, särskilt i fråga om utbyte av information mellan myndigheter som är ansvariga för förebyggande och utredning av brott. Beslutet innehåller därför regler på följande områden:

a) Bestämmelser om villkoren och förfarandet för automatisk överföring av DNA-profiler, fingeravtrycksuppgifter och vissa uppgifter ur nationella fordonsregister (kapitel 2).

b) Bestämmelser om villkoren för översändande av uppgifter i samband med större evenemang med gränsöverskridande verkningar (kapitel 3).

c) Bestämmelser om villkoren för översändande av uppgifter för förebyggande av terroristbrott (kapitel 4).

d) Bestämmelser om villkoren och förfarandet för fördjupat gränsöverskridande polissamarbete genom olika åtgärder (kapitel 5).

KAPITEL 2

ÅTKOMST ON-LINE OCH BEGÄRAN OM UPPFÖLJNING

AVSNITT 1

DNA-profiler

Artikel 2

Inrättande av nationella databaser med DNA-analyser

1. Medlemsstaterna ska inrätta och upprätthålla nationella databaser med DNA-analyser för brottsutredningar. Behandlingen av uppgifter i dessa databaser inom ramen för detta beslut ska utföras i enlighet med detta beslut, i överensstämmelse med nationell rätt som är tillämplig på behandlingen.

2. För genomförandet av detta beslut ska medlemsstaterna se till att det i överensstämmelse med punkt 1 första meningen bereds tillgång till referensuppgifterna i de nationella databaserna med DNA-analyser. Referensuppgifterna ska endast innehålla DNA-profiler från den icke-kodifierande delen av DNA:t och en sifferbeteckning. Referensuppgifterna får inte innehålla uppgifter som möjliggör en omedelbar identifiering av den berörda personen. Referensuppgifter, som inte är kopplade till en viss person (oidentifierade DNA-profiler), ska kunna identifieras som sådana.

3. Varje medlemsstat ska underrätta rådets generalsekretariat om de nationella databaser med DNA-analyser på vilka artiklarna 2–6 kan tillämpas samt villkoren förutsättningarna för automatisk sökning som avses i artikel 3.1 i enlighet med artikel 36.

Artikel 3

Automatisk sökning av DNA-profiler

1. I samband med brottsutredningar ska medlemsstaterna ge de övriga medlemsstaternas nationella kontaktställen enligt artikel 6 tillträde till referensuppgifterna i sina databaser med DNA-profiler med rätt att göra automatiska sökningar i dem genom jämförelse av DNA-profiler. Sökningen får endast göras i enskilda fall och i överensstämmelse med den nationella lagstiftningen i den ansökande medlemsstaten.

2. Om det i samband med en automatisk sökning konstateras att en förmedlad DNA-profil motsvarar DNA-profiler i den mottagande medlemsstatens databas, ska det nationella kontaktstället i den ansökande medlemsstaten automatiskt ta emot de referensuppgifter för vilka överensstämmelse har konstaterats. Om ingen överensstämmelse konstateras ska detta meddelas automatiskt.

Artikel 4

Automatisk jämförelse av DNA-profiler

1. Medlemsstaterna ska i samband med brottsutredningar enligt en gemensam överenskommelse genom sina nationella kontaktställen jämföra DNA-profilerna för sina egna oidentifierade DNA-profiler med referensuppgifterna för alla övriga parters nationella databaser med DNA-analyser. Profilerna ska översändas och jämföras automatiskt. Oidentifierade DNA-profiler ska översändas för jämförelse endast i sådana fall där den ansökande medlemsstatens nationella lagstiftning tillåter det.

2. Om en medlemsstat till följd av en jämförelse enligt punkt 1 konstaterar att en översänd DNA-profil motsvarar en profil som ingår i någon av dess egna databaser med DNA-profiler ska den utan dröjsmål tillställa den andra medlemsstatens nationella kontaktställe de referensuppgifter för vilka överensstämmelse har konstaterats.

Artikel 5

Översändande av övriga personuppgifter och ytterligare information

Om en överensstämmelse mellan DNA-profiler konstateras vid förfaranden enligt artiklarna 3 och 4 ska översändande av övriga tillgängliga personuppgifter och ytterligare information med anknytning till referensuppgifterna regleras av den anmodade medlemsstatens nationella lagstiftning, inklusive bestämmelserna om rättshjälp.

Artikel 6

Nationellt kontaktställe och genomförandeåtgärder

1. Varje medlemsstat ska utse ett nationellt kontaktställe för förmedling av de uppgifter som avses i artiklarna 3 och 4. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

2. De tekniska detaljerna för det förfarande som beskrivs i artiklarna 3 och 4 ska fastställas i de genomförandeåtgärder som avses i artikel 33.

Artikel 7

Insamling av molekylärgenetiskt material och översändande av DNA-profiler

Om det under pågående brottsutredning eller straffrättsliga förfaranden saknas en DNA-profil över en viss person som vistas i en anmodad medlemsstat, ska den medlemsstaten ge rättshjälp genom att insamla och undersöka molekylärgenetiskt material från denna person och översända den DNA-profil som erhållits, om

a) den ansökande medlemsstaten meddelar för vilket ändamål detta behövs,

b) den ansökande medlemsstaten i enlighet med sin lagstiftning framställer en begäran eller ett förordnande om undersökning från den behöriga myndigheten, där det framgår att det hade funnits förutsättningar för insamling och undersökning av molekylärgenetiskt material om personen i fråga hade vistats i den ansökande medlemsstaten, och

c) det enligt lagstiftningen i den anmodade medlemsstaten finns förutsättningar för insamling och undersökning av molekylärgenetiskt material samt för översändande av den DNA-profil som erhålls.

AVSNITT 2

Fingeravtrycksuppgifter

Artikel 8

Fingeravtrycksuppgifter

För genomförandet av detta beslut ska medlemsstaterna se till att referensuppgifterna i de för brottsförebyggande och brottsutredning inrättade nationella systemen för automatisk identifiering av fingeravtryck hålls tillgängliga. Referensuppgifterna ska endast innehålla fingeravtrycksuppgifter och en sifferbeteckning. Referensuppgifterna får inte innehålla uppgifter som möjliggör en omedelbar identifiering av den berörda personen. Referensuppgifter som inte är kopplade till en viss person ("oidentifierade fingeravtrycksuppgifter") ska kunna identifieras som sådana.

Artikel 9

Automatisk sökning av fingeravtrycksuppgifter

1. För förebyggande och utredning av brott ska medlemsstaterna ge de övriga medlemsstaternas nationella kontaktställen enligt artikel 11 tillträde till referensuppgifterna i de system för automatisk identifiering av fingeravtryck som inrättats för detta syfte och ska ge dem rätt att göra automatiska sökningar i dem genom jämförelse av fingeravtrycksuppgifter. Sökningen får endast göras i enskilda fall och i överensstämmelse med den nationella lagstiftningen i den ansökande medlemsstaten.

2. Bekräftelse av fingeravtrycksuppgifters överensstämmelse med referensuppgifterna hos den medlemsstat som administrerar databasen ska utföras av det nationella kontaktstället i den ansökande medlemsstaten genom att de referensuppgifter som krävs för att säkerställa en entydig överensstämmelse översänds automatiskt.

Artikel 10

Översändande av övriga personuppgifter och ytterligare information

Om en överensstämmelse mellan fingeravtrycksuppgifter konstateras vid ett förfarande enligt artikel 9 ska översändandet av övriga personuppgifter och ytterligare information med anknytning till referensuppgifterna regleras av den anmodade medlemsstatens nationella lagstiftning, inklusive bestämmelserna om rättslig hjälp.

Artikel 11

Nationellt kontaktställe och genomförandeåtgärder

1. Varje medlemsstat ska utse ett nationellt kontaktställe för förmedling av de uppgifter som avses i artikel 9. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

2. De tekniska detaljerna för det förfarande som anges i artikel 9 ska fastställas i de genomförandeåtgärder som avses i artikel 33.

AVSNITT 3

Uppgifter ur fordonsregister

Artikel 12

Automatisk sökning av uppgifter ur fordonsregister

1. För förebyggande och utredning av brott samt för undersökning av sådana överträdelser som i den ansökande medlemsstaten lyder under domstols- och åklagarväsendets behörighet samt för upprätthållande av allmän säkerhet ska medlemsstaterna ge övriga medlemsstaters nationella kontaktställen enligt punkt 2 tillträde till följande uppgifter i de nationella fordonsregistren, med rätt att i enskilda fall göra automatiska sökningar:

a) Uppgifter om ägare och innehavare.

b) Uppgifter om fordonet.

En sökning får endast genomföras genom användning av ett fordons fullständiga chassinummer eller fullständiga registreringsnummer. Sökningar får endast göras i överensstämmelse med den ansökande medlemsstatens nationella lagstiftning.

2. Varje medlemsstat ska för förmedling av de uppgifter som avses i punkt 1 utse ett nationellt kontaktställe som tar emot förfrågningar. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen. De tekniska detaljerna för förfarandet ska fastställas i de genomförandeåtgärder som avses i artikel 33.

KAPITEL 3

STÖRRE EVENEMANG

Artikel 13

Översändande av andra uppgifter än personuppgifter

För förebyggande av brott och upprätthållande av allmän ordning och säkerhet i samband med större evenemang med gränsöverskridande verkningar, såsom betydande idrottsevenemang eller Europeiska rådets möten, ska medlemsstaterna både på begäran och på eget initiativ i överensstämmelse med den översändande medlemsstatens nationella lagstiftning sända varandra nödvändiga icke personrelaterade uppgifter.

Artikel 14

Översändande av personuppgifter

1. För förebyggande bekämpning av brott och upprätthållande av allmän ordning och säkerhet i samband med större evenemang med gränsöverskridande verkningar, såsom betydande idrottsevenemang eller Europeiska rådets möten, ska medlemsstaterna både på begäran och på eget initiativ sända varandra personuppgifter, om det på grundval av domar som vunnit laga kraft eller andra fakta finns skäl att anta att personerna i fråga kommer att begå brott vid de berörda evenemangen eller att personerna utgör ett hot mot den allmänna ordningen och säkerheten, förutsatt att översändande av sådana uppgifter är tillåtet enligt den nationella lagstiftningen i den medlemsstat som sänder uppgifterna.

2. Personuppgifter får endast behandlas för de syften som avses i punkt 1 och endast i samband med de evenemang för vilket de har översänts. De uppgifter som har översänts ska utplånas omedelbart när de syften som avses i punkt 1 har uppnåtts eller när de inte längre kan uppnås. De uppgifter som översänts ska under alla omständigheter utplånas senast inom ett år.

Artikel 15

Nationellt kontaktställe

Varje medlemsstat ska utse ett nationellt kontaktställe för förmedling av de uppgifter som avses i artiklarna 13 och 14. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

KAPITEL 4

ÅTGÄRDER FÖR FÖREBYGGANDE AV TERRORISTBROTT

Artikel 16

Översändande av uppgifter för bekämpning av terroristbrott

1. Medlemsstaterna får i överensstämmelse med nationell lagstiftning och i enskilda fall, även utan föregående förfrågan, för förebyggande av terroristbrott översända personuppgifter och andra uppgifter enligt punkt 2 till de övriga medlemsstaternas nationella kontaktställen enligt punkt 3, i den mån det är nödvändigt därför att särskilda omständigheter ger anledning att anta att de berörda personerna kommer att göra sig skyldiga till sådana brott som avses i artiklarna 1–3 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism [1].

[1] EGT L 164, 22.6.2002, s. 3.

2. De uppgifter som ska översändas är efternamn, förnamn, födelsetid och födelseort samt en beskrivning av de omständigheter som ligger till grund för det antagande som avses i punkt 1.

3. Varje medlemsstat ska utse ett nationellt kontaktställe för utbyte av information med övriga medlemsstaters nationella kontaktställen. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

4. Den översändande medlemsstaten kan i enlighet med den nationella lagstiftningen fastställa de villkor enligt vilka den mottagande medlemsstaten får använda sådana uppgifter. Dessa villkor ska vara bindande för den mottagande medlemsstaten.

KAPITEL 5

ANDRA FORMER AV SAMARBETE

Artikel 17

Gemensamma insatser

1. För att fördjupa polissamarbetet kan de behöriga myndigheter som medlemsstaterna utser, för upprätthållande av allmän ordning och säkerhet samt för förebyggande av brott, inrätta gemensamma patruller och genomföra andra gemensamma insatser där utsedda tjänstemän eller andra statsanställda (nedan kallade *tjänstemän*) från andra medlemsstater deltar i insatser på en annan medlemsstats territorium.

2. Varje medlemsstat får i egenskap av värdmedlemsstat, i enlighet med sin nationella lagstiftning och med den utsändande medlemsstatens medgivande, ge tjänstemän från de utsändande medlemsstaterna rätt att utöva verkställande befogenheter i samband med gemensamma insatser eller, när detta är tillåtet enligt värdmedlemsstatens lagstiftning, bevilja de utsändande medlemsstaternas tjänstemän rätt att utöva verkställande befogenheter i enlighet med den utsändande medlemsstatens lagstiftning. Sådana verkställande befogenheter får endast utövas under överinsyn av och i regel i närvaro av värdmedlemsstatens tjänstemän. De utsändande medlemsstaternas tjänstemän ska lyda under värdmedlemsstatens nationella lagstiftning. Värdmedlemsstaten ska ansvara för deras handlingar.

3. Tjänstemän från utsändande medlemsstater som deltar i gemensamma insatser ska iaktta de anvisningar som meddelas av värdmedlemsstatens behöriga myndighet.

4. Medlemsstaterna ska lämna förklaringar enligt artikel 36 i vilka de fastställer de praktiska aspekterna av samarbetet.

Artikel 18

Bistånd vid större evenemang, katastrofer och allvarliga olyckor

Medlemsstaternas behöriga myndigheter ska ge varandra ömsesidigt bistånd i enlighet med sin nationella lagstiftning vid större evenemang, och liknande viktiga händelser, katastrofer och allvarliga olyckor, genom att försöka förhindra brott och upprätthålla allmän ordning och säkerhet, genom att

a) i ett så tidigt skede som möjligt underrätta varandra om sådana situationer som har gränsöverskridande verkningar, och förmedla väsentliga uppgifter som hänför sig till dem,

b) i situationer med gränsöverskridande verkningar genomföra och samordna nödvändiga polisiära åtgärder på sitt territorium,

c) på begäran av den medlemsstat på vars territorium situationen i fråga har uppstått, i den mån det är möjligt, ge bistånd genom att sända tjänstemän, specialister och rådgivare samt genom att ställa övrig nödvändig utrustning till förfogande.

Artikel 19

Användning av tjänstevapen, ammunition och övrig nödvändig utrustning

1. En utsändande medlemsstats tjänstemän som inom ramen för en gemensam insats vistas på en annan medlemsstats territorium enligt artikel 17 eller 18 får använda sin nationella tjänsteuniform. De får inneha tjänstevapen, ammunition och övrig nödvändig utrustning i enlighet med den utsändande medlemsstatens nationella lagstiftning. Värdmedlemsstaten får förbjuda den utsändande medlemsstatens tjänstemän att medföra vissa tjänstevapen, viss ammunition eller utrustning.

2. Medlemsstaterna ska lämna förklaringar enligt artikel 36 i vilka de förtecknar de tjänstevapen, den ammunition och utrustning som endast får användas vid nödvärn för att skydda sig själv eller andra. Värdmedlemsstatens tjänsteman som leder insatsen kan i enskilda fall i enlighet med den nationella lagstiftningen godkänna användning av tjänstevapen, ammunition och utrustning i andra fall än de som avses i första meningen. Vid användning av tjänstevapen, ammunition och övrig nödvändig utrustning ska värdmedlemsstatens lagstiftning iakttas. De behöriga myndigheterna ska underrätta varandra om tillåtna tjänstevapen och tillåten ammunition och utrustning och villkoren för användningen av dem.

3. Om en medlemsstats tjänstemän i samband med åtgärder i enlighet med detta beslut använder motorfordon på en annan medlemsstats territorium, ska för dem gälla samma trafikbestämmelser som för värdmedlemsstatens tjänstemän, inklusive de bestämmelser om skyldighet att lämna företräde och särskilda rättigheter i vägtrafiken.

4. Medlemsstaterna ska lämna förklaringar enligt artikel 36 i vilka de fastställer de praktiska aspekterna i samband med användningen av tjänstevapen, ammunition och utrustning.

Artikel 20

Skydd och bistånd

Medlemsstaterna ska vara skyldiga att skydda och bistå andra medlemsstaters tjänstemän som överskrider gränserna på samma sätt som sina egna tjänstemän.

Artikel 21

Allmänna bestämmelser om skadeståndsansvar

1. När en medlemsstats tjänstemän verkar i en annan medlemsstat i enlighet med artikel 17, ska deras medlemsstat ansvara för de eventuella skador som de förorsakar under sina insatser, i enlighet med lagstiftningen i den medlemsstat på vars territorium de verkar.

2. Den medlemsstat på vars territorium de skador som avses i punkt 1 förorsakades ska ersätta sådana skador enligt de villkor som gäller för skador som förorsakas av dess egna tjänstemän.

3. I det fall som anges i punkt 1 ska den medlemsstat vars tjänstemän har förorsakat skador på någon person på en annan medlemsstats territorium till fullo ersätta den andra medlemsstaten för alla belopp den har betalat ut till offren eller de personer som befullmäktigats att handla på offrens vägnar.

4. När en medlemsstats tjänstemän verkar i en annan medlemsstat i enlighet med artikel 18, ska den sistnämnda medlemsstaten i enlighet med sin nationella lagstiftning ansvara för de eventuella skador som de förorsakar under sina insatser.

5. När den skada som avses i punkt 4 följer av grov oaktsamhet eller avsiktlig försummelse, får värdmedlemsstaten begära att hemmedlemsstaten ska ersätta de belopp som värdmedlemsstaten har betalat ut för att gottgöra offren eller de personer som på offrens vägnar har rätt till ersättning.

6. Utan att det påverkar utövandet av eventuella rättigheter gentemot tredje part och med undantag för vad som sägs i punkt 3 ska alla medlemsstater under de omständigheter som avses i punkt 1 avstå från att kräva ersättning för de skador den lidit av en annan medlemsstat.

Artikel 22

Straffrättsligt ansvar

Tjänstemän som enligt detta beslut verkar på en annan medlemsstats territorium ska i fråga om brott som de begår eller brott som de utsätts för jämställas med den andra medlemsstatens tjänstemän, om inte annat följer av något annat avtal som är bindande för de berörda medlemsstaterna.

Artikel 23

Tjänsteförhållanden

Tjänstemän som enligt detta beslut verkar på en annan medlemsstats territorium ska i tjänsterättsligt hänseende, särskilt vad gäller de disciplinära bestämmelserna, omfattas av den tillämpliga lagstiftningen i sin egen medlemsstat.

KAPITEL 6

ALLMÄNNA BESTÄMMELSER OM DATASKYDD

Artikel 24

Definitioner och tillämpningsområde

1. I detta beslut gäller följande definitioner:

a) *behandling av personuppgifter*: all behandling av personuppgifter eller en räcka behandlingar med eller utan hjälp av automatiska förfaranden, såsom insamling, registrering, organisering, lagring, bearbetning eller ändring, urval, förfrågan, konsultering, användning, överlåtelse genom överföring, spridning och alla andra former av tillhandahållande, kombination eller sammankoppling samt spärrande, avförande eller utplånande av uppgifter. Som behandling av personuppgifter enligt detta beslut anses även underrättelse om huruvida en överensstämmelse konstaterats eller inte.

b) *automatisk sökning*: direkt tillträde till ett annat organs automatiska databas på ett sätt där en förfrågan besvaras fullständigt automatiskt.

c) *förseende med en beteckning*: märkning av registrerade personuppgifter som inte syftar till att begränsa den framtida behandlingen av dem.

d) *spärrande*: märkning av registrerade personuppgifter i syfte att begränsa den framtida behandlingen av dem.

2. Följande bestämmelser ska gälla för uppgifter som översänds eller har översänts enligt detta beslut, om inte annat föreskrivs i de föregående kapitlen.

Artikel 25

Dataskyddsnivå

1. Varje medlemsstat ska i sin nationella lagstiftning, i fråga om behandlingen av personuppgifter som översänds eller har översänts enligt detta beslut, garantera ett skydd för personuppgifter som motsvarar åtminstone den nivå som fastställs i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter och i tilläggsprotokollet av den 8 november 2001, och ska därvid beakta rekommendation nr R (87) 15 av den 17 september 1987 från Europarådets ministerkommitté till medlemsstaterna om polisens användning av personuppgifter, även när uppgifterna inte behandlas automatiskt.

2. Översändande av personuppgifter i enlighet med detta beslut får inledas först när bestämmelserna i detta kapitel har genomförts i lagstiftningen i de medlemsstater som deltar i informationsutbytet. Rådet ska enhälligt besluta om huruvida denna förutsättning är uppfylld.

3. Punkt 2 ska inte tillämpas på de medlemsstater där översändandet av personuppgifter enligt detta beslut redan har inletts i enlighet med fördraget av den 27 maj 2005 mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration (Prümfördraget).

Artikel 26

Syfte

1. Den mottagande medlemsstaten får behandla personuppgifter endast för de syften för vilka uppgifterna har översänts i enlighet med detta beslut. Behandling för andra syften ska vara tillåten endast med förhandstillstånd från den medlemsstat som administrerar uppgifterna och i enlighet med den mottagande medlemsstatens nationella lagstiftning. Ett sådant tillstånd får beviljas om den nationella lagstiftningen i den medlemsstat som administrerar uppgifterna tillåter denna behandling för sådana andra syften.

2. Den sökande eller jämförande medlemsstaten får behandla uppgifter som översänts i enlighet med artiklarna 3, 4 och 9 endast för

a) fastställande av om jämförda DNA-profiler eller fingeravtrycksuppgifter överensstämmer,

b) utarbetande och inlämnande av en begäran om handräckning eller rättslig hjälp i enlighet med den nationella lagstiftningen när dessa uppgifter överensstämmer,

c) registrering i enlighet med artikel 30.

Den medlemsstat som administrerar uppgifterna får behandla uppgifter som översänts till den i enlighet med artiklarna 3, 4 och 9 endast om det är nödvändigt för att göra en jämförelse, svara på en automatisk sökning eller göra en registrering enligt artikel 30. Efter det att jämförelsen av uppgifter avslutats eller den automatiska sökningen besvarats ska de uppgifter som översänts omedelbart utplånas, om det inte är nödvändigt med en ytterligare behandling av dem för de syften som anges i leden b och c i första stycket.

3. Den medlemsstat som administrerar uppgifterna får använda uppgifter som översänts i enlighet med artikel 12 endast om det är nödvändigt för besvarande av en automatisk sökning eller för registrering i enlighet med artikel 30. Efter det att den automatiska sökningen besvarats ska de uppgifter som översänts omedelbart utplånas, om det inte är nödvändigt med en ytterligare behandling av dem för registrering i enlighet med artikel 30. Den sökande medlemsstaten får använda de uppgifter som erhållits under sökningen endast för det förfarande på grundval av vilket sökningen skett.

Artikel 27

Behöriga myndigheter

Översända personuppgifter får endast behandlas av de myndigheter, organ och domstolar som ansvarar för en uppgift i enlighet med syftena i artikel 26. Särskilt får uppgifter översändas till andra myndigheter endast med den översändande medlemsstatens förhandstillstånd och i enlighet med den mottagande medlemsstatens nationella lagstiftning.

Artikel 28

Uppgifternas korrekthet, aktualitet och lagringstid

1. Medlemsstaterna ska säkerställa att personuppgifterna är korrekta och aktuella. Om det *ex officio* eller genom ett meddelande från den berörda personen visar sig att felaktiga uppgifter eller uppgifter som inte borde ha översänts har översänts, ska den eller de mottagande medlemsstaterna omedelbart underrättas om detta. Den eller de berörda medlemsstaterna ska vara skyldiga att rätta eller utplåna uppgifterna. Även i övriga fall ska översända personuppgifter rättas om det framgår att de är felaktiga. Om det mottagande organet har skäl att anta att de översända uppgifterna är felaktiga eller bör utplånas ska den utan dröjsmål underrätta det översändande organet om detta.

2. Uppgifter vars korrekthet den berörda personen bestrider och vars korrekthet eller felaktighet inte kan fastställas ska märkas, i enlighet med medlemsstaternas nationella lagstiftning, på begäran av den person som uppgifterna berör. Om en sådan märkning har använts får denna avlägsnas, i enlighet med medlemsstaternas nationella lagstiftning, endast med den berörda personens medgivande eller genom beslut av en behörig domstol eller en oberoende myndighet som ansvarar för övervakningen av dataskyddet.

3. Översända personuppgifter ska utplånas om de inte borde ha översänts eller mottagits. Uppgifter som har översänts och mottagits korrekt ska utplånas

a) om de inte eller inte längre är nödvändiga för det syfte för vilket de översänts; om personuppgifterna har översänts utan begäran ska det mottagande organet omedelbart kontrollera om de är nödvändiga med tanke på de syften för vilka de översändes,

b) efter det att den tidsfrist som fastställs för lagring av uppgifterna enligt den översändande medlemsstatens nationella lagstiftning har löpt ut, när det översändande organet har informerat det mottagande organet om denna maximala lagringstid i samband med att uppgifterna översändes.

I stället för att utplånas ska uppgifterna spärras i enlighet med den nationella lagstiftningen om det finns skäl att anta att en utplåning skulle skada den berörda personens intressen. Spärrade uppgifter får endast översändas eller användas i det syfte som lett till att utplåningen förhindrades.

Artikel 29

Tekniska och organisatoriska åtgärder för säkerställande av dataskydd och datasäkerhet

1. De översändande och mottagande organen ska vidta åtgärder så att personuppgifter skyddas effektivt mot oavsiktlig eller otillåten utplåning, oavsiktlig förlust, obehörig tillgång, obehörig eller oavsiktlig ändring och obehörigt offentliggörande.

2. Detaljerna för det automatiska sökningsförfarandet ska fastställas i de genomförandeåtgärder som avses i artikel 33, som garanterar att

a) åtgärder som motsvarar den senaste tekniken vidtas för att säkerställa dataskydd och datasäkerhet, särskilt uppgifternas konfidentialitet och integritet,

b) krypterings- och autentiseringsmetoder som erkänns av de behöriga myndigheterna används när allmänt tillgängliga nät utnyttjas, och

c) det i enlighet med artikel 30.2, 30.4 och 30.5 kan kontrolleras att sökningarna är tillåtna.

Artikel 30

Registrering och dokumentation, särskilda bestämmelser om automatiskt och icke-automatiskt översändande

1. Varje medlemsstat ska garantera att varje icke-automatiskt översändande och varje icke-automatiskt mottagande av personuppgifter i det organ som administrerar databasen och i det sökande organet registreras för att kontrollera att sändningen är tillåten. Registreringen ska omfatta följande uppgifter:

a) Skälet till översändandet.

b) Översända uppgifter.

c) Datum för översändandet.

d) Namn eller sifferbeteckning på det sökande organet och det organ som administrerar databasen.

2. För automatisk sökning av uppgifter i enlighet med artiklarna 3, 9 och 12 och för automatisk jämförelse i enlighet med artikel 4 ska följande gälla:

a) En automatisk sökning eller jämförelse får endast genomföras av de tjänstemän vid nationella kontaktställen som särskilt bemyndigats att göra detta. En förteckning över de tjänstemän som bemyndigats att genomföra automatiska sökningar eller jämförelser ska på begäran ställas till förfogande för de övervakningsmyndigheter som avses i punkt 5 och de övriga medlemsstaterna.

b) Varje medlemsstat ska garantera att varje översändande och mottagande av personuppgifter i det organ som administrerar databasen och i det sökande organet registreras tillsammans med uppgift om huruvida sökningen lett till en träff eller inte. Denna registrering ska omfatta följande uppgifter:

i) Översända uppgifter.

ii) Datum och exakt tidpunkt för översändandet.

iii) Namn eller sifferbeteckning på det sökande organet och det organ som administrerar databasen.

Det sökande organet ska dessutom registrera sökningens eller översändandets syfte samt en identitetsuppgift för den tjänsteman som initierade sökningen eller översändandet.

3. Det registrerande organet ska på begäran utan dröjsmål delge den berörda medlemsstatens behöriga dataskyddsmyndigheter de registrerade uppgifterna, dock senast fyra veckor efter det att begäran inkom. De registrerade uppgifterna får endast användas för följande ändamål:

a) Övervakning av dataskydd.

b) Garanterande av datasäkerheten.

4. De registrerade uppgifterna ska med hjälp av lämpliga åtgärder skyddas mot obehörig användning och andra former av missbruk och lagras i två år. När lagringstiden har löpt ut ska de registrerade uppgifterna utan dröjsmål utplånas.

5. Den rättsliga övervakningen av översändande och mottagande av personuppgifter ska ankomma på de oberoende dataskyddsmyndigheterna eller, i förekommande fall, de rättsliga myndigheterna i varje medlemsstat. I enlighet med den nationella lagstiftningen kan var och en hos dessa myndigheter ansöka om en granskning av lagligheten beträffande behandlingen av sina personuppgifter. Dessa myndigheter och de organ som ansvarar för registreringen ska även oberoende av ovan nämnda ansökningar göra stickprov för att kontrollera översändningarnas laglighet med hjälp av berörda dokument.

De oberoende dataskyddsmyndigheterna ska förvara resultaten av dessa kontroller för granskning i 18 månader. Efter denna tidsfrist ska de utplånas omedelbart. Varje dataskyddsmyndighet kan anmodas av den oberoende dataskyddsmyndigheten i en annan medlemsstat att utöva sina befogenheter i enlighet med den nationella lagstiftningen. Medlemsstaternas oberoende dataskyddsmyndigheter ska utföra de inspektioner som är nödvändiga för det ömsesidiga samarbetet, särskilt genom utbyte av relevant information.

Artikel 31

Berörda personers rätt till information och skadestånd

1. På begäran av den berörda personen i enlighet med nationell lagstiftning ska denna person som bevisar sin identitet, utan oskäliga avgifter, i en allmänt förståelig form och utan oacceptabla dröjsmål, i enlighet med nationell lagstiftning informeras om de uppgifter om denna person som har varit föremål för behandling, liksom om uppgifternas ursprung, mottagare eller kategori av mottagare, det avsedda ändamålet med behandlingen och, när så krävs i nationell lagstiftning, dess rättsliga grund. Dessutom ska den person som uppgifterna berör ha rätt att kräva att felaktiga uppgifter korrigeras och att uppgifter som behandlats på otillbörligt sätt utplånas. Medlemsstaterna ska dessutom säkerställa att den person som uppgifterna berör, då personens rättigheter avseende dataskydd kränkts, kan överklaga hos en oavhängig domstol enligt artikel 6.1 i den europeiska konventionen om de mänskliga rättigheterna eller hos en oberoende tillsynsmyndighet enligt artikel 28 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter [1], och att personen ges möjlighet att kräva skadestånd eller annan ersättning. De närmare bestämmelserna för förfarandet för att hävda dessa rättigheter och skälen till begränsning av tillgången ska följa den tillämpliga nationella lagstiftningen i den medlemsstat där personen i fråga hävdar sina rättigheter.

2. När ett organ i en medlemsstat har översänt personuppgifter i enlighet med detta beslut, kan den mottagande myndigheten i en annan medlemsstat inte hänvisa till att de översända uppgifterna var felaktiga för att undgå sitt ansvar gentemot den skadelidande i enlighet med den nationella lagstiftningen. Om det mottagande organet döms att betala skadestånd på grund av dess användning av översända felaktiga uppgifter ska det översändande organet ersätta det mottagande organets skadeståndsbetalning till fullt belopp.

Artikel 32

Information på begäran av medlemsstaterna

Den mottagande medlemsstaten ska på begäran ge den översändande medlemsstaten information om behandlingen av de översända uppgifterna och de resultat som erhållits.

KAPITEL 7

GENOMFÖRANDE OCH SLUTBESTÄMMELSER

Artikel 33

Genomförandeåtgärder

Rådet ska, med kvalificerad majoritet och efter att ha hört Europaparlamentet, besluta om de åtgärder som är nödvändiga för att genomföra detta beslut på unionsnivå.

Artikel 34

Kostnader

Varje medlemsstat ska ansvara för de driftskostnader som dess egna myndigheter ådrar sig i samband med tillämpningen av detta beslut. I särskilda fall får de berörda medlemsstaterna komma överens om avvikande arrangemang.

Artikel 35

Förhållandet till andra instrument

1. För de berörda medlemsstaterna ska de tillämpliga bestämmelserna i detta beslut tillämpas i stället för motsvarande bestämmelser i Prümfördraget. Varje annan bestämmelse i Prümfördraget ska fortfarande vara tillämplig mellan de fördragsslutande parterna i Prümfördraget.

2. Medlemsstaterna får, utan att det påverkar deras åtaganden enligt andra rättakter som antagits enligt avdelning VI i fördraget,

a) fortsätta att tillämpa bilaterala eller multilaterala avtal eller överenskommelser om gränsöverskridande samarbete som är i kraft den dag då detta beslut antas, förutsatt att dessa avtal eller överenskommelser inte är oförenliga med målen för detta beslut,

b) ingå eller låta träda i kraft bilaterala eller multilaterala avtal eller överenskommelser om gränsöverskridande samarbete efter det att detta beslut har trätt i kraft, förutsatt att dessa avtal eller överenskommelser gör det möjligt att utvidga eller bredda målen för detta beslut.

3. De avtal och överenskommelser som avses i punkterna 1 och 2 får inte påverka förbindelserna med de medlemsstater som inte är parter i dem.

4. Medlemsstaterna ska inom fyra veckor efter det att detta beslut fått verkan underrätta rådet och kommissionen om de befintliga avtal eller överenskommelser enligt punkt 2 a som de vill fortsätta att tillämpa.

5. Medlemsstaterna ska också underrätta rådet och kommissionen om alla nya avtal eller överenskommelser enligt punkt 2 b inom tre månader efter undertecknandet eller, om det gäller instrument som undertecknades innan detta beslut antogs, inom tre månader efter deras ikraftträdande.

6. Ingenting i detta beslut ska påverka bilaterala eller multilaterala avtal eller överenskommelser mellan medlemsstaterna och tredjestater.

7. Detta beslut ska inte påverka befintliga avtal om rättslig hjälp eller ömsesidigt erkännande av domstolsavgöranden.

[1] EGT L 281, 23.11.1995, s. 31. Direktivet ändrat genom förordning (EG) nr 1882/2003 (EUT L 284, 31.10.2003, s. 1.)

Artikel 36

Genomförande och förklaringar

1. Medlemsstaterna ska vidta nödvändiga åtgärder för att följa bestämmelserna i detta beslut inom ett år efter det att beslutet har fått verkan, med undantag av bestämmelserna i kapitel 2 avseende vilka nödvändiga åtgärder ska vidtas inom tre år efter det att detta beslut och rådets beslut om tillämpningen av detta beslut har fått verkan.

2. Medlemsstaterna ska underrätta rådets generalsekretariat och kommissionen om att de har uppfyllt de skyldigheter som de åläggs enligt detta beslut och lämna in de förklaringar som avses i beslutet. I samband med detta får varje medlemsstat meddela att den omedelbart kommer att tillämpa detta beslut i förbindelserna med de medlemsstater som har lämnat samma meddelande.

3. Förklaringar som har lämnats i enlighet med punkt 2 får när som helst ändras genom en förklaring som lämnas till rådets generalsekretariat. Rådets generalsekretariat ska vidarebefordra alla mottagna förklaringar till medlemsstaterna och kommissionen.

4. På grundval av detta och annan information som medlemsstaterna gjort tillgänglig på begäran ska kommissionen inge en rapport till rådet senast den 28 juli 2012 om genomförandet av detta beslut åtföljd av förslag som den anser lämpliga för vidare utveckling.

Artikel 37

Tillämpning

Detta beslut får verkan tjugo dagar efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Luxemburg den 23 juni 2008.

På rådets vägnar

I. JARC

Ordförande

RÅDETS BESLUT 2008/616/RIF av den 23 juni 2008 om genomförande av beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet

L 210/12 SV Europeiska unionens officiella tidning 6.8.2008

RÅDETS BESLUT 2008/616/RIF

av den 23 juni 2008

om genomförande av beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet

EUROPEISKA UNIONENS RÅD HAR BESLUTAT FÖLJANDE

med beaktande av artikel 33 i rådets beslut 2008/615/RIF [1],

med beaktande av initiativet från Förbundsrepubliken Tyskland,

med beaktande av Europaparlamentets yttrande [2], och

av följande skäl:

(1) Den 23 juni 2008 antog rådet beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet.

(2) Genom beslut 2008/615/RIF införlivades de väsentliga delarna av fördraget av den 27 maj 2005 mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration (nedan kallat *Prümfördraget*) med Europeiska unionens rättsliga ram.

(3) Enligt artikel 33 i beslut 2008/615/RIF ska rådet besluta om de åtgärder som är nödvändiga för att genomföra beslut 2008/615/RIF på unionsnivå i enlighet med förfarandet i artikel 34.2 c andra meningen i fördraget om Europeiska unionen. Dessa åtgärder ska bygga på genomförandeavtalet av den 5 december 2006 beträffande de administrativa och tekniska aspekterna av genomförandet och tillämpningen av Prümfördraget.

(4) I beslutet fastställs de gemensamma normativa bestämmelser som är absolut nödvändiga för det administrativa och tekniska genomförandet av de samarbetsformer som anges i beslut 2008/615/RIF. Bilagan till det här beslutet innehåller genomförandebestämmelser av teknisk karaktär. En separat handbok, som endast innehåller faktauppgifter som ska lämnas av medlemsstaterna, kommer dessutom att utarbetas och hållas uppdaterad av rådets generalsekretariat.

(5) Med beaktande av de tekniska resurserna kommer rutinsökningar av nya DNA-profiler i princip att genomföras med hjälp av enstaka sökningar och lämpliga lösningar för detta kommer att sökas på teknisk nivå.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte

Syftet med detta beslut är att fastställa de nödvändiga administrativa och tekniska bestämmelserna för genomförandet av beslut 2008/615/RIF, särskilt för det automatiska utbytet av DNA-uppgifter, fingeravtryckuppgifter och uppgifter ur fordonsregister enligt kapitel 2 i det beslutet samt för andra samarbetsformer enligt kapitel 5 i det beslutet.

Artikel 2

Definitioner

I detta beslut gäller följande definitioner

a) *sökning* och *jämförelse* enligt artiklarna 3, 4 och 9 i beslut 2008/615/RIF: de förfaranden genom vilka det fastställs om det finns någon överensstämmelse mellan DNA-uppgifter eller fingeravtryckuppgifter som har lämnats av en medlemsstat och DNA-uppgifter eller fingeravtryckuppgifter som finns lagrade i en, flera eller samtliga medlemsstaters databaser.

b) *automatisk sökning* enligt artikel 12 i beslut 2008/615/RIF: förfarande för tillgång online för att söka i en, flera eller samtliga medlemsstaters databaser.

c) *DNA-profil*: en bokstav eller en nummerkod som representerar en rad identifikationsuppgifter i den icke-kodifierande delen av ett analyserat mänskligt DNA-prov, dvs. den särskilda molekylära strukturen vid de olika DNA-lokusen.

d) *icke-kodifierande del av DNA*: kromosomområden som inte innehåller någon genetisk information, dvs. inga hänvisningar till en organisms funktionella egenskaper.

[1] Se sidan 1 i detta nummer av EUT.
[2] Yttrandet avgivet den 21 april 2008 (ännu ej offentliggjort i EUT).

e) *DNA-referensuppgifter*: en DNA-profil och en sifferbeteckning.

f) *DNA-personprofil*: DNA-profilen för en identifierad person.

g) *oidentifierad DNA-profil*: den DNA-profil som erhålls från spår som samlats in under brottsutredningen och tillhör en person som ännu inte identifierats.

h) *notering*: en medlemsstats markering i en DNA-profil i den nationella databasen om att man redan konstaterat en överensstämmelse för en sådan DNA-profil vid en annan medlemsstats sökning eller jämförelse.

i) *fingeravtrycksuppgifter*: fingeravtrycksbilder, dolda fingeravtrycksbilder, handavtryck, dolda handavtryck samt modeller för sådana bilder (kodade detaljer), när de lagras och hanteras i en automatisk databas.

j) *uppgifter ur fordonsregister*: uppsättningen uppgifter enligt kapitel 3 i bilagan till detta beslut.

k) *enskilda fall* enligt artiklarna 3.1 andra meningen, 9.1 andra meningen och 12.1 i beslut 2008/615/RIF: en enda utrednings- eller lagföringsfil. Om en sådan fil innehåller mer än en DNA-profil, fingeravtrycksuppgift eller uppgift ur fordonsregister ska dessa översändas tillsammans som en begäran.

KAPITEL 2

GEMENSAMMA BESTÄMMELSER OM UTBYTE AV UPPGIFTER

Artikel 3

Tekniska specifikationer

Medlemsstaterna ska följa de gemensamma tekniska specifikationerna i samband med varje begäran och svar som gäller sökningar och jämförelser av DNA-profiler, fingeravtrycksuppgifter och uppgifter ur fordonsregister. Dessa tekniska specifikationer fastställs i bilagan till detta beslut.

Artikel 4

Kommunikationsnät

Det elektroniska utbytet av DNA-uppgifter, fingeravtrycksuppgifter och uppgifter ur fordonsregister mellan medlemsstaterna ska ske med hjälp av kommunikationsnätet för de transeuropeiska tjänsterna för telematik mellan förvaltningarnas (Testa II) och vidareutveckling av dessa.

Artikel 5

Tillgång till automatiskt utbyte av uppgifter

Medlemsstaterna ska vidta alla nödvändiga åtgärder för att säkerställa att automatisk sökning eller jämförelse av DNA-uppgifter, fingeravtrycksuppgifter och uppgifter ur fordonsregister är möjlig dygnet runt sju dagar i veckan. Vid tekniskt fel ska medlemsstaternas nationella kontaktpunkter omedelbart underrätta varandra och enas om system för tillfälligt alternativt informationsutbyte i enlighet med de tillämpliga rättsliga bestämmelserna. Automatiskt utbyte av uppgifter ska återupprättas så snabbt som möjligt.

Artikel 6

Sifferbeteckningar för DNA-uppgifter och fingeravtrycksuppgifter

De sifferbeteckningar som avses i artiklarna 2 och 8 i beslut 2008/615/RIF ska bestå av en kombination av följande:

a) En kod som gör det möjligt för medlemsstaterna att om en överensstämmelse konstaterats hämta personuppgifter och ytterligare information från sina databaser för vidarebefordran till en, flera eller samtliga medlemsstater i enlighet med artikel 5 eller artikel 10 i beslut 2008/615/RIF.

b) En kod för att ange DNA-profilens eller fingeravtrycksuppgifternas nationella ursprung.

c) För DNA-uppgifter, en kod för att ange typen av DNA-profil.

KAPITEL 3

DNA-UPPGIFTER

Artikel 7

Principer för utbyte av DNA-uppgifter

1. Medlemsstaterna ska använda befintliga standarder för utbyte av DNA-uppgifter, till exempel den europeiska standarduppsättningen (ESS) eller Interpols standarduppsättning med lokus (Issol).

2. Översändandet ska vid automatisk sökning och jämförelse av DNA-uppgifter ske inom en decentraliserad struktur.

3. Lämpliga åtgärder ska vidtas för att säkerställa konfidentialiteten och integriteten för de uppgifter som översänds till andra medlemsstater, inklusive krypteringen av dessa.

4. Medlemsstaterna ska vidta nödvändiga åtgärder för att garantera integriteten för de DNA-profiler som görs tillgängliga eller skickas för jämförelse till de andra medlemsstaterna och säkerställa att dessa åtgärder överensstämmer med internationella standarder, exempelvis ISO 17025.

5. Medlemsstaterna ska använda medlemsstatskoder enligt ISO-standarden 3166-1 tvåbokstavskod.

Artikel 8

Regler för begäran och svar i samband med DNA-uppgifter

1. En begäran om en automatisk sökning eller jämförelse enligt artikel 3 eller 4 i beslut 2008/615/RIF ska endast innehålla följande information:

a) Den begärande medlemsstatens medlemsstatskod.

b) Dag, tid och referensnummer för begäran.

c) DNA-profiler och deras sifferbeteckning.

d) Typer av DNA-profiler som har översänts (oidentifierade DNA-profiler eller DNA-personprofiler).

e) Information som krävs för att kontrollera databassystemen och kvalitetskontroll för de automatiska sökprocesserna.

2. Svaret (rapporten om de automatiska sökprocesserna överensstämmelse) på en begäran enligt punkt 1 ska endast innehålla följande information:

a) Uppgift om det finns ett eller flera fall av överensstämmelse (träffar) eller inte (ingen träff).

b) Dag, tid och referensnummer för begäran.

c) Dag, tid och referensnummer för svaret.

d) De begärande och de anmodade medlemsstaternas medlemsstatskoder.

e) De begärande och de anmodade medlemsstaternas sifferbeteckningar.

f) Den typ av DNA-profiler som översänds (oidentifierade DNA-profiler eller DNA-personprofiler).

g) De begärda och överensstämmande DNA-profilerna.

h) Information som krävs för att kontrollera databassystemen och kvalitetskontroll för de automatiska sökprocesserna.

3. En överensstämmelse ska meddelas automatiskt endast om den automatiska sökningen eller jämförelsen har resulterat i en överensstämmelse mellan ett minimiantal lokus. Detta minimiantal fastställs i kapitel 1 i bilagan till detta beslut.

4. Medlemsstaterna ska se till att begäran överensstämmer med de förklaringar som lämnats enligt artikel 2.3 i beslut 2008/615/RIF. Förklaringarna ska återges i den handbok som avses i artikel 18.2 i detta beslut.

Artikel 9

Översändandeförfarande för automatisk sökning av oidentifierade DNA-profiler i enlighet med artikel 3 i beslut 2008/615/RIF

1. Om man vid en sökning med en oidentifierad DNA-profil inte har konstaterat någon överensstämmelse i den nationella databasen, eller man har konstaterat överensstämmelse med en oidentifierad DNA-profil, får den oidentifierade DNA-profilen översändas till alla övriga medlemsstaters databaser, och om man vid en sökning med denna oidentifierade DNA-profil konstaterar överensstämmelser med DNA-personprofiler och/eller oidentifierade DNA-profiler i andra medlemsstaters databaser, ska dessa överensstämmelser automatiskt meddelas och DNA-referensuppgifterna översändas till den begärande medlemsstaten. Om man inte kan konstatera någon överensstämmelse i andra medlemsstaters databaser, ska detta automatiskt meddelas den begärande medlemsstaten.

2. Om man vid en sökning med en oidentifierad DNA-profil konstaterar en överensstämmelse i andra medlemsstaters databaser får varje berörd medlemsstat föra in en notering om detta i sin nationella databas.

Artikel 10

Översändandeförfarande för automatisk sökning av DNA-personprofiler i enlighet med artikel 3 i beslut 2008/615/RIF

Om man vid en sökning med en DNA-personprofil inte har konstaterat någon överensstämmelse i den nationella databasen med en DNA-personprofil eller konstaterat en överensstämmelse med en oidentifierad DNA-profil, får denna DNA-personprofil översändas till alla övriga medlemsstaters databaser, och om man vid en sökning med denna DNA-personprofil konstaterar överensstämmelser med DNA-personprofiler och/eller oidentifierade DNA-profiler i andra medlemsstaters databaser ska dessa överensstämmelser automatiskt meddelas och DNA-referensuppgifterna översändas till den begärande medlemsstaten. Om man inte kan konstatera någon överensstämmelse i andra medlemsstaters databaser, ska detta automatiskt meddelas den begärande medlemsstaten.

Artikel 11

Översändandeförfarande för automatisk jämförelse av oidentifierade DNA-profiler i enlighet med artikel 4 i beslut 2008/615/RIF

1. Om man vid en jämförelse med oidentifierade DNA-profiler konstaterar överensstämmelser med DNA-personprofiler och/eller oidentifierade DNA-profiler i andra medlemsstaters databaser ska dessa överensstämmelser automatiskt meddelas och DNA-referensuppgifterna översändas till den begärande medlemsstaten.

2. Om man vid en jämförelse med oidentifierade DNA-profiler konstaterar överensstämmelser med oidentifierade DNA-profiler eller DNA-personprofiler i andra medlemsstaters databaser får varje berörd medlemsstat införa en notering om detta i sin nationella databas.

KAPITEL 4

FINGERAVTRYCKSUPPGIFTER

Artikel 12

Principer för utbyte av fingeravtrycksuppgifter

1. Digitalisering av fingeravtrycksuppgifter och översändandet av dessa till de övriga medlemsstaterna ska genomföras i enlighet med ett enhetligt dataformat som specificeras i kapitel 2 i bilagan till detta beslut.

2. Varje medlemsstat ska se till att de fingeravtrycksuppgifter som den översänder har tillräckligt god kvalitet för att kunna jämföras med hjälp av de automatiska fingeravtrycksidentifieringssystemen (Afis).

3. Översändandeförfarandet för utbyte av fingeravtrycksuppgifter ska ske inom en decentraliserad struktur.

4. Lämpliga åtgärder ska vidtas för att säkerställa konfidentialiteten och integriteten för de fingeravtrycksuppgifter som översänds till andra medlemsstater, inklusive krypteringen av dessa.

5. Medlemsstaterna ska använda medlemsstatskoder i enlighet med ISO-standard 3166-1 tvåbokstavskod.

Artikel 13

Sökningskapacitet för fingeravtrycksuppgifter

1. Varje medlemsstat ska se till att dess begäran om sökning inte överskrider den sökningskapacitet som specificerats av den anmodade medlemsstaten. Medlemsstaterna ska lämna förklaringar som anges i artikel 18.2 till rådets generalsekretariat i vilka de fastställer sin maximala sökningskapacitet per dag för fingeravtrycksuppgifter om identifierade personer eller för fingeravtrycksuppgifter om ännu inte identifierade personer.

2. Det maximala antalet personer som godtas för kontroll per översändande fastställs i kapitel 2 i bilagan till detta beslut.

Artikel 14

Regler för begäran och svar i samband med fingeravtrycksuppgifter

1. Den anmodade medlemsstaten ska utan dröjsmål kontrollera kvaliteten på de översända fingeravtrycksuppgifterna genom ett helt automatiskt förfarande. Om uppgifterna inte lämpar sig för en automatisk jämförelse, ska den anmodade medlemsstaten omedelbart underrätta den begärande medlemsstaten.

2. Den anmodade medlemsstaten ska utföra sökningar i den ordning som den får begäran. Begäran ska behandlas inom 24 timmar genom ett helt automatiskt förfarande. Den begärande medlemsstaten får, om dess nationella lagstiftning så föreskriver, begära att behandlingen av dess begäran påskyndas och den anmodade medlemsstaten ska utföra dessa sökningar utan dröjsmål. Om tidsfristerna inte kan hållas på grund av *force majeure,* ska jämförelsen göras utan dröjsmål så snart som hindren har avlägsnats.

KAPITEL 5

UPPGIFTER UR FORDONSREGISTER

Artikel 15

Principer för automatisk sökning av uppgifter ur fordonsregister

1. För automatisk sökning av uppgifter ur fordonsregister ska medlemsstaterna använda en enligt artikel 12 i beslut 2008/615/RIF särskilt utarbetad version av programvaran för det europeiska informationssystemet avseende fordon och körkort (Eucaris) och ändrade versioner av denna programvara.

2. Automatisk sökning av uppgifter ur fordonsregister ska ske inom en decentraliserad struktur.

3. De uppgifter som utbyts via Eucaris-systemet ska översändas i krypterad form.

4. De delar av uppgifterna ur fordonsregistret som ska utbytas specificeras i kapitel 3 i bilagan till detta beslut.

5. Vid tillämpningen av artikel 12 i beslut 2008/615/RIF får medlemsstaterna prioritera sökningar i syfte att bekämpa allvarlig brottslighet.

Artikel 16

Kostnader

Varje medlemsstat ska ansvara för kostnaderna för administrationen, användningen och underhållet av den version av programvaran för Eucaris som anges i artikel 15.1.

KAPITEL 6

POLISSAMARBETE

Artikel 17

Gemensam patrullering och andra gemensamma insatser

1. Enligt kapitel 5 i beslut 2008/615/RIF, särskilt de förklaringar som lämnats enligt artiklarna 17.4, 19.2 och 19.4 i det beslutet, ska varje medlemsstat utse en eller flera kontaktpunkter

så att andra medlemsstater kan vända sig till de behöriga myndigheterna och varje medlemsstat får specificera sina förfaranden för att inleda gemensam patrullering och andra gemensamma insatser, sina förfaranden för initiativ från andra medlemsstater när det gäller dessa insatser samt andra praktiska aspekter och operativa regler i samband med dessa insatser.

2. Rådets generalsekretariat ska sammanställa och uppdatera en förteckning över kontaktpunkterna och underrätta de behöriga myndigheterna om eventuella ändringar i förteckningen.

3. De behöriga myndigheterna i varje medlemsstat får ta initiativ till att inleda en gemensam insats. Innan en specifik insats inleds, ska de behöriga myndigheter som avses i punkt 2 skriftligen eller muntligen vidta arrangemang som till exempel kan avse

a) de behöriga myndigheterna i de medlemsstater som ansvarar för insatsen,

b) insatsens specifika syfte,

c) den värdmedlemsstat där insatsen äger rum,

d) det geografiska området i den värdmedlemsstat där insatsen äger rum,

e) den period som insatsen avser,

f) det särskilda bistånd som den utsändande medlemsstaten/de utsändande medlemsstaterna ska tillhandahålla värdmedlemsstaten, bl.a. tjänstemän eller andra statsanställda, materiel och finansiella inslag,

g) de tjänstemän som deltar i insatsen,

h) den tjänsteman som leder insatsen,

i) de befogenheter som den utsändande medlemsstatens/de utsändande medlemsstaternas tjänstemän eller andra statsanställda får utöva i värdmedlemsstaten under insatsen,

j) vissa tjänstevapen, viss ammunition och utrustning som de utsända tjänstemännen får använda under insatsen enligt beslut 2008/615/RIF,

k) regler för logistiken kring transport, inkvartering och säkerhet,

l) ansvaret för kostnaderna för den gemensamma insatsen vid avvikelse från vad som föreskrivs i artikel 34 första meningen i beslut 2008/615/RIF,

m) eventuella övriga inslag som krävs.

4. De förklaringar, förfaranden och utseenderegler som föreskrivs i denna artikel ska återges i den handbok som avses i artikel 18.2.

KAPITEL 7

SLUTBESTÄMMELSER

Artikel 18

Bilaga och handbok

1. Ytterligare uppgifter om det tekniska och administrativa genomförandet av beslut 2008/615/RIF återfinns i bilagan till det här beslutet.

2. En handbok ska utarbetas och hållas uppdaterad av rådets generalsekretariat samt endast innehålla faktauppgifter som lämnas av medlemsstaterna genom förklaringar i enlighet med beslut 2008/615/RIF eller det här beslutet eller genom anmälningar till rådets generalsekretariat. Handboken ska ha formen av ett rådsdokument.

Artikel 19

Oberoende dataskyddsmyndigheter

Medlemsstaterna ska, i enlighet med artikel 18.2 i detta beslut, informera rådets generalsekretariat om de oberoende dataskyddsmyndigheter eller de rättsliga myndigheter som avses i artikel 30.5 i beslut 2008/615/RIF.

Artikel 20

Förberedelse av beslut enligt artikel 25.2 i beslut 2008/615/RIF

1. Rådet ska fatta ett beslut enligt artikel 25.2 i beslut 2008/615/RIF på grundval av en utvärderingsrapport som ska grundas på ett frågeformulär.

2. Med beaktande av det automatiska utbytet av uppgifter i enlighet med kapitel 2 i beslut 2008/615/RIF ska utvärderingsrapporten även grundas på ett utvärderingsbesök och en testkörning som ska genomföras när den berörda medlemsstaten har informerat generalsekretariatet enligt artikel 36.2 första meningen i beslut 2008/615/RIF.

3. Närmare uppgifter om förfarandet anges i kapitel 4 i bilagan till detta beslut.

Artikel 21

Utvärdering av utbytet av uppgifter

1. En utvärdering av den administrativa, tekniska och finansiella tillämpningen av utbytet av uppgifter enligt kapitel 2 i beslut 2008/615/RIF, särskilt användningen av mekanismen i artikel 15.5, ska genomföras regelbundet. Utvärderingen ska omfatta de medlemsstater som redan tillämpar beslut 2008/615/RIF vid tiden för utvärderingen och beakta de uppgiftskategorier för

vilka utbytet av uppgifter har inletts bland de berörda medlemsstaterna. Utvärderingen ska grundas på de respektive medlemsstaternas rapporter.

2. Närmare uppgifter om förfarandet anges i kapitel 4 i bilagan till detta beslut.

Artikel 22

Förhållandet till genomförandeavtalet till Prümfördraget

För de medlemsstater som är bundna av Prümfördraget ska de tillämpliga bestämmelserna i detta beslut och dess bilaga – så snart de har genomförts fullt ut – tillämpas i stället för motsvarande bestämmelser i genomförandeavtalet till Prümfördraget. Varje annan bestämmelse i Prümfördraget ska fortfarande vara tillämplig mellan de fördragsslutande parterna i Prümfördraget.

Artikel 23

Genomförande

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att följa bestämmelserna i detta beslut inom de tidsfrister som avses i artikel 36.1 i beslut 2008/615/RIF.

Artikel 24

Tillämpning

Detta beslut får verkan tjugo dagar efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Luxemburg den 23 juni 2008.

På rådets vägnar

I. JARC

Ordförande

BILAGA

INNEHÅLLSFÖRTECKNING

KAPITEL 1: **Utbyte av DNA-uppgifter**

1. ***DNA-relaterade kriminaltekniska frågor, matchningsregler och algoritmer***

1.1 *DNA-profilernas egenskaper*

DNA-profilen kan innehålla 24 talpar som representerar allelerna i 24 lokus som också används vid Interpols DNA-förfaranden. Benämningarna för dessa lokus framgår av följande tabell:

VWA	TH01	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenin
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	FES	F13A1	F13B	SE33	CD4	GABA

De sju gråmarkerade lokusen i den översta raden utgör både den nuvarande europeiska standarduppsättningen av lokus (ESS) och Interpols standarduppsättning av lokus (Issol).

Inklusionsregler:

De DNA-profiler som medlemsstaterna gör tillgängliga för sökning och jämförelse samt de DNA-profiler som sänds för sökning och jämförelse måste innehålla minst 6 fullständigt angivna [1] lokus och får innehålla ytterligare lokus eller tomma positioner beroende på tillgång. DNA-personprofiler måste innehålla minst 6 av de 7 ESS-lokusen. För att öka noggrannheten vid matchningen ska alla tillgängliga alleler lagras i den indexerade databasen med DNA-profiler och användas för sökning och jämförelse. Varje medlemsstat ska så snart det är praktiskt möjligt tillämpa varje ny ESS-lokus som antas av EU.

Blandade profiler är inte tillåtna, vilket gör att allel-värdena för varje lokus består av endast två tal. Vid homozygositet kan dessa tal vara lika för ett givet lokus.

Jokertecken och mikrovarianter ska behandlas enligt följande regler:

— Varje icke-numeriskt värde utom amelogenin som profilen innehåller (t.ex. "o", "f", "r", "na", "nr" eller "un") måste automatiskt konverteras till ett jokertecken (*) vid exporten och sökas mot alla.

— De numeriska värdena "0", "1" or "99" i profilen måste automatiskt konverteras till ett jokertecken (*) vid exporten och sökas mot alla.

— Om 3 alleler ges för ett lokus ska den första allelen godtas och de återstående 2 måste automatiskt konverteras till ett jokertecken (*) vid exporten och sökas mot alla.

— Om jokertecken ges för allel 1 eller 2 ska båda permutationerna av det numeriska värdet för lokuset sökas ("12,*" kan till exempel matcha "12,14" eller "9,12").

— Mikrovarianter av pentanukleotider (Penta D, Penta E och CD4) ska matchas på följande sätt:

x.1 = x, x.1, x.2

x.2 = x.1, x.2, x.3

x.3 = x.2, x.3, x.4

x.4 = x.3, x.4, x + 1

— Mikrovarianter av tetranukleotider (övriga lokus är tetranukleotider) ska matchas på följande sätt:

x.1 = x, x.1, x.2

x.2 = x.1, x.2, x.3

x.3 = x.2, x.3, x + 1

[1] "Fullständigt angivna" betyder att hantering av ovanliga alleler inkluderas.

1.2 *Matchningsregler*

Jämförelsen av två DNA-profiler ska göras på grundval av de lokus för vilka ett par allelvärden är tillgängliga i båda DNA-profilerna. Minst 6 fullständigt angivna lokus (exklusive amelogenin) måste överensstämma mellan de två DNA-profilerna innan ett träffsvar ges.

Full överensstämmelse (*Quality 1*) definieras som en överensstämmelse där samtliga allelvärden är identiska för de jämförda lokus som finns både i den DNA-profil som används för sökningen och i den sökta DNA-profilen. Nära överensstämmelse definieras som en överensstämmelse där värdet för endast en av samtliga jämförda alleler skiljer sig mellan de två DNA-profilerna (*Quality 2*, 3 och 4). En nära överensstämmelse godtas endast om det finns minst 6 fullständigt angivna lokus med full överensstämmelse i de två jämförda DNA-profilerna.

Anledningen till en nära överensstämmelse kan vara

— ett skrivfel vid inmatningen av en av DNA-profilerna i sökningen eller i DNA-databasen,

— ett fel vid allelbestämningen eller allelanropet under förfarandet för generering av DNA-profilen.

1.3 *Rapporteringsregler*

Både fulla överensstämmelser, nära överensstämmelser och "inga träffar" ska rapporteras.

Överensstämmelserapporten ska sändas till den begärande nationella kontaktpunkten samt göras tillgänglig för den tillfrågade nationella kontaktpunkten (så att den kan uppskatta arten av och antal eventuella uppföljande begäranden om ytterligare personuppgifter och annan information med anknytning till den DNA-profil som svarar mot träffen i enlighet med artiklarna 5 och 10 i beslut 2008/615/RIF).

2. ***Tabell över medlemsstatskoder***

I enlighet med beslut 2008/615/RIF, används ISO 3166-1 tvåställiga bokstavskoder för att upprätta domännamn och andra konfigurationsparametrar som krävs för Prümtillämpningarna för utbyte av DNA-uppgifter via ett slutet nät.

De tvåställiga medlemsstatskoderna enligt ISO 3166-1 alpha-2 är följande:

Medlemsstatens namn	Kod	Medlemsstatens namn	Kod
Belgien	BE	Luxemburg	LU
Bulgarien	BG	Ungern	HU
Tjeckien	CZ	Malta	MT
Danmark	DK	Nederländerna	NL
Tyskland	DE	Österrike	AT
Estland	EE	Polen	PL
Grekland	EL	Portugal	PT
Spanien	ES	Rumänien	RO
Frankrike	FR	Slovakien	SK
Irland	IE	Slovenien	SI
Italien	IT	Finland	FI
Cypern	CY	Sverige	SE
Lettland	LV	Förenade kungariket	UK
Litauen	LT		

3. ***Funktionsanalys***

3.1 *Systemets tillgänglighet*

En begäran om sökning enligt artikel 3 i beslut 2008/615/RIF bör nå den anropade databasen i kronologisk ankomstordning enligt vilken begäran sändes, medan svaren bör nå den anmodande medlemsstaten inom 15 minuter efter det att begäran inkom.

3.2 *Steg 2*

När en medlemsstat mottar en rapport om överensstämmelse ansvarar den nationella kontaktpunkten för en jämförelse mellan värdena i den profil som sänds som fråga och värdena i den profil/de profiler som har mottagits som svar i syfte att validera och kontrollera profilens bevisvärde. De nationella kontaktpunkterna kan ta direktkontakter i valideringssyfte.

Förfaranden för rättslig hjälp inleds efter det att en överensstämmelse mellan två profiler validerats, på grundval av "fullständig överensstämmelse" eller "nära överensstämmelse" under det automatiska sökningsförfarandet.

4. ***Dokument för gränssnittskontroll – DNA***

4.1 *Inledning*

4.1.1 Syfte

Detta kapitel anger kraven för informationsutbytet om DNA-profiler mellan samtliga medlemsstaters DNA-databassystem. Fälten i huvudet är specificerade speciellt för Prüm-utbytet av DNA-uppgifter och datadelen grundar sig på datadelen för DNA-uppgifter enligt XML-schemat för Interpols nätport för utbyte av DNA-uppgifter.

Uppgifterna utbyts genom SMTP (Simple Mail Transfer Protocol) med användning av en central e-postserver som ställs till förfogande av nätoperatören. XML-filen överförs som meddelandetext.

4.1.2 Omfattning

Detta dokument för gränssnittskontroll, ICD, rör endast e-postmeddelandets innehåll. Alla nätspecifika och e-postspecifika områden definieras på ett likartat sätt för att ge en gemensam teknisk grund för utbytet av DNA-uppgifter.

Detta inbegriper

— formatet för meddelandets ärendefält, så att meddelandena kan bearbetas automatiskt,

— specifikationer av huruvida kryptering erfordras och i så fall vilka metoder som bör väljas,

— maximilängd för meddelandena.

4.1.3 XML-struktur och XML-principer

XML-meddelandet är indelat i

— ett huvud som innehåller information om överföringen, och

— en datadel som innehåller profilspecifik information samt själva profilen.

Samma XML-schema ska kunna användas för både begäran och svar.

För fullständiga kontroller av oidentifierade DNA-profiler (artikel 4 i beslut 2008/615/RIF) ska det vara möjligt att sända en uppsättning profiler i ett enda meddelande. Det maximala antalet profiler i ett meddelande måste fastställas. Detta antal är beroende av den maximala meddelandestorleken och ska fastställas efter val av e-postserver.

XML-exempel:

<?version="1.0" standalone="yes"?>

<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<header>

(…)

</header>

<datas>

(…)

</datas>

[<datas> datastrukturen upprepas om fler än en profil sänds i (....) ett enda SMTP-meddelande, något som endast tillåts i fall enligt artikel 4

</datas>

</PRUEMDNA>

4.2 *Definition av XML-strukturen*

Följande definitioner medtas endast i dokumentationssyfte och för bättre läsbarhet, den faktiskt bindande informationen återfinns i en fil med XML-schemat (PRUEM DNA.xsd).

4.2.1 Specifikation PRUEMDNAx

Den innehåller följande fält:

Fields	Type	Description
header	PRUEM_header	Occurs: 1
datas	PRUEM_datas	Occurs: 1 ... 500

4.2.2 Innehåll i huvudfältets struktur

4.2.2.1 PRUEM-huvud

Denna struktur beskriver XML-filhuvudet. Den innehåller följande fält:

Fields	Type	Description
direction	PRUEM_header_dir	Direction of message flow
ref	String	Reference of the XML file
generator	String	Generator of XML file
schema_version	String	Version number of schema to use
requesting	PRUEM_header_info	Requesting Member State info
requested	PRUEM_header_info	Requested Member State info

4.2.2.2 PRUEM_header dir

Typ av data i meddelandet, värden

Value	Description
R	Request

Value	Description
A	Answer

4.2.2.3 Information i PRUEM-huvudet

Struktur som beskriver medlemsstaten samt anger datum och tid för meddelandet. Den innehåller följande fält:

Fields	Type	Description
source_isocode	String	ISO 3166-2 code of the requesting Member State
destination_isocode	String	ISO 3166-2 code of the requested Member State
request_id	String	unique Identifier for a request
date	Date	Date of creation of message
time	Time	Time of creation of message

4.2.3 PRUEM-profiluppgifter, innehåll

4.2.3.1 PRUEM_datas

Denna struktur beskriver XML-profilens datadel: Den innehåller följande fält:

Fields	Type	Description
reqtype	PRUEM request type	Type of request (Article 3 or 4)
date	Date	Date profile stored
type	PRUEM_datas_type	Type of profile
result	PRUEM_datas_result	Result of request
agency	String	Name of corresponding unit responsible for the profile
profile_ident	String	Unique Member State profile ID
message	String	Error Message, if result = E
profile	IPSG_DNA_profile	If direction = A (Answer) AND result ≠ H (Hit) empty
match_id	String	In case of a HIT PROFILE_ID of the requesting profile
quality	PRUEM_hitquality_type	Quality of Hit
hitcount	Integer	Count of matched Alleles
rescount	Integer	Count of matched profiles. If direction = R (Request), then empty. If quality!=0 (the original requested profile), then empty.

4.2.3.2 PRUEM_request_type

Typ av data i meddelandet, värden:

Value	Description
3	Requests pursuant to Article 3 of Decision 2008/615/JHA
4	Requests pursuant to Article 4 of Decision 2008/615/JHA

4.2.3.3 PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: Case "No Hit": original requesting profile sent back only; Case "Hit": original requesting profile and matched profiles sent back.
1	Equal in all available alleles without wildcards
2	Equal in all available alleles with wildcards
3	Hit with Deviation (Microvariant)
4	Hit with mismatch

4.2.3.4 PRUEM_data_type

Typ av data i meddelandet, värden:

Value	Description
P	Person profile
S	Stain

4.2.3.5 PRUEM_data_result

Typ av data i meddelandet, värden:

Value	Description
U	Undefined, If direction = R (request)
H	Hit
N	No Hit
E	Error

4.2.3.6 IPSG_DNA_profile

Struktur som beskriver en DNA-profil. Den innehåller följande fält:

Fields	Type	Description
ess_issol	IPSG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSG_DNA_additional_loci	Other loci
marker	String	Method used to generate of DNA
profile_id	String	Unique identifier for DNA profile

4.2.3.7 IPSG_DNA_ISSOL

Struktur som innehåller Issol-lokus (Interpols standarduppsättning lokus). Den innehåller följande fält:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

Fields	Type	Description
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogin

4.2.3.8 IPSG_DNA_additional_loci

Struktur som innehåller övriga lokus. Den innehåller följande fält:

Fields	Type	Description
tpox	IPSG_DNA_locus	Locus tpox
csf1po	IPSG_DNA_locus	Locus csf1po
d13s317	IPSG_DNA_locus	Locus d13s317
d7s820	IPSG_DNA_locus	Locus d7s820
d5s818	IPSG_DNA_locus	Locus d5s818
d16s539	IPSG_DNA_locus	Locus d16s539
d2s1338	IPSG_DNA_locus	Locus d2s1338
d19s433	IPSG_DNA_locus	Locus d19s433
penta_d	IPSG_DNA_locus	Locus penta_d
penta_e	IPSG_DNA_locus	Locus penta_e
fes	IPSG_DNA_locus	Locus fes
f13a1	IPSG_DNA_locus	Locus f13a1
f13b	IPSG_DNA_locus	Locus f13b
se33	IPSG_DNA_locus	Locus se33
cd4	IPSG_DNA_locus	Locus cd4
gaba	IPSG_DNA_locus	Locus gaba

4.2.3.9 IPSG_DNA_locus

Struktur som beskriver ett lokus. Den innehåller följande fält:

Fields	Type	Description
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

5. ***Tillämpnings-, säkerhets- och kommunikationsarkitektur***

5.1 *Översikt*

Vid införandet av tillämpningar för utbyte av DNA-uppgifter inom ramen för beslut 2008/615/RIF ska ett gemensamt, på logisk nivå slutet, nät mellan medlemsstaterna användas. För att mer effektivt utnyttja detta

gemensamma kommunikationsnät för att sända begäranden och ta emot svar ska begäranden om DNA- och fingeravtrycksuppgifter överföras asynkront i inkapslade SMTP-meddelanden. Av hänsyn till säkerhetskraven kommer S/MIME-mekanismen att användas som tillägg till SMTP-funktionerna för att upprätta en obruten säker tunnel i nätet.

Det redan fungerande systemet Testa (Trans European Services for Telematics between Administrations) har valts som kommunikationsnät för datautbytet mellan medlemsstaterna. Europeiska kommissionen ansvarar för närvarande för Testa. Eftersom de nationella DNA-databaserna och de nuvarande nationella anslutningspunkterna för Testa kan vara belägna på olika ställen i medlemsstaterna kan tillgång till Testa anordnas antingen

1) genom att använda den befintliga nationella anslutningspunkten eller inrätta en ny nationell anslutningspunkt till Testa, eller

2) genom att etablera en säker lokal länk, från den plats där DNA-databasen finns och förvaltas av det behöriga nationella organet, till den befintliga nationella anslutningspunkten till Testa.

De protokoll och standarder som används vid införandet av tillämpningar enligt beslut 2008/615/RIF står i överensstämmelse med öppna standarder och uppfyller de kraven från dem som ansvarar för medlemsstaternas nationella säkerhet.

5.2 *Högnivåarkitektur*

Enligt beslut 2008/615/RIF ska varje medlemsstat göra sin DNA-databas tillgänglig för utbyte med och/eller sökning från andra medlemsstater i enlighet med ett standardiserat gemensamt dataformat. Arkitekturen bygger på kommunikationsmodellen alla-till-alla (*any-to-any*). Det finns ingen central server och inte heller någon centraliserad databas med DNA-profiler.

Figur 1: Topologi över utbyte av DNA-uppgifter

Medlemsstaterna ska iaktta de nationella rättsliga restriktionerna för medlemsstaternas webbplatser och kan också bestämma vilken typ av hårdvara och vilka program som bör användas för att konfigurera medlemsstatens webbplats för att iaktta kraven i beslut 2008/615/RIF.

5.3 *Säkerhetsstandarder och dataskydd*

Tre nivåer av säkerhetsklassning har övervägts och införts.

5.3.1 Datanivån

De DNA-profiluppgifter som tillhandahålls av varje medlemsstat måste utformas i enlighet med en gemensam standard för dataskydd så att den begärande medlemsstaten får ett svar som huvudsakligen anger TRÄFF eller ICKE-TRÄFF samt vid TRÄFF ett identifikationsnummer som inte innehåller några som helst personuppgifter. Den fortsatta undersökningen efter meddelande om TRÄFF kommer att genomföras på bilateral nivå i enlighet med de nationella rättsliga och organisatoriska föreskrifter som gäller vid respektive medlemsstats anläggning.

5.3.2 Kommunikationsnivån

Meddelanden som innehåller information om DNA-profiler (begäranden och svar) kommer att krypteras med senaste teknik, anpassad till öppna standarder, t.ex. S/MIME, innan de översänds till andra medlemsstaters anläggningar.

5.3.3 Transmissionsnivån

Alla krypterade meddelanden med DNA-profilinformation kommer att vidarebefordras till andra medlemsstaters anläggningar genom ett virtuellt privat tunnelsystem som på internationell nivå förvaltas av en tillförlitlig nätleverantör och med nationellt ansvar för de säkra länkarna till detta tunnelsystem. Det virtuella privata tunnelsystemet har ingen anslutning till det öppna Internet.

5.4 *Protokoll och standarder för krypteringsmekanismen S/MIME och därmed sammanhörande paket*

Den öppna standarden S/MIME, en vidareutveckling av den faktiska e-poststandarden SMTP, kommer att användas för att kryptera meddelanden med DNA-profilinformation. Protokollet S/MIME (version 3) ger möjlighet till signerade kvittenser, säkerhetsuppmärkning och säkra sändlistor på grundval av en kryptografisk meddelandestandard (*Cryptographic Message Syntax*, CMS), en specifikation från *Internet Engineering Task Force* (IETF) för meddelanden skyddade genom kryptering. Det kan användas för att digitalt signera, autentisera eller kryptera alla former av uppgifter i digital form.

Det certifikat som S/MIME-mekanismen använder måste överensstämma med X.509-standarden. För att se till att de gemensamma standarderna och förfarandena överensstämmer med andra Prüm-tillämpningar gäller följande regler för S/MIME-kryptering eller i samband med olika Cots-miljöer (Cots, färdigköpt allmänt tillgänglig produkt).

— Bearbetningsordning: Först kryptering, därefter signering.

— Krypteringsalgoritmerna AES (*Advanced Encryption Standard*) med 256 bitars nyckellängd och RSA med 1 024 bitars nyckellängd ska användas för symmetrisk respektive asymmetrisk kryptering.

— Hash-algoritmen SHA-1 ska användas.

S/MIME-funktioner finns i de allra flesta moderna programpaket för e-post, bland annat Outlook, Mozilla Mail och Netscape Communicator 4.x och är interoperabla mellan alla viktigare programpaket för e-post.

S/MIME har valts som lämplig mekanism för dataskyddet på kommunikationsnivån eftersom den är lätt att införliva i den nationella infrastrukturen vid alla medlemsstaters anläggningar. För att på ett effektivare sätt och till lägre kostnader visa hur tekniken fungerar har dock den öppna standarden JavaMail API valts för prototypen till utbytet av DNA-uppgifter. JavaMail API erbjuder enkel kryptering och dekryptering av e-postmeddelanden med användning av S/MIME och/eller OpenPGP. Avsikten är att erbjuda ett enkelt och lättanvänt API för e-postkunder som vill sända och ta emot e-post i något av de två mest populära formaten för krypterade e-postmeddelanden. Därför är det tillräckligt med någon av de senaste tillämpningarna av *JavaMail API* för de krav som ställs i beslut 2008/615/RIF, t.ex. en produkt från *Bouncy Castle JCE (Java Cryptographic Extension)*, som kommer att användas för tillämpningen av S/MIME för prototypen av utbytet av DNA-uppgifter mellan alla medlemsstater.

5.5 *Tillämpningsarkitektur*

Varje medlemsstat kommer att ge övriga medlemsstater en uppsättning standardiserade DNA-profiluppgifter som är anpassade till gällande dokument för gränssnittskontroll (*Interface Control Document, ICD*). Detta kan antingen göras genom en logisk visning av den enskilda nationella databasen eller genom att upprätta en fysiskt exporterad databas (indexerad databas).

De fyra huvuddelarna: E-postservern/S/MIME, tillämpningsservern, datastrukturområdet för hämtning/inmatning av uppgifter och registrering av inkommande/utgående meddelanden samt matchningsmotorn genomför tillämpningslogiken på ett produktoberoende sätt.

För att alla medlemsstater lätt ska kunna införliva dessa komponenter i sina respektive anläggningar har de specificerade gemensamma funktionerna införts genom öppna standarder och protokoll som varje medlemsstat själv kan välja med hänsyn till nationell IT-policy och nationella IT-föreskrifter. På grund av de oberoende funktioner som ska införas för att få tillgång till de indexerade DNA-profildatabaser som omfattas av beslut 2008/615/RIF kan varje medlemsstat fritt välja plattform för hårdvara och program, inklusive databas- och operativsystem.

En prototyp för utbytet av DNA-uppgifter har utarbetats och prövats med framgång på det befintliga gemensamma nätet. Version 1.0 har utnyttjats i produktionsmiljö och används för det löpande arbetet. Medlemsstaterna får använda den produkt som har utvecklats gemensamt men får också utveckla egna produkter. De gemensamma produktkomponenterna kommer att bevaras, anpassas och vidareutvecklas i enlighet med de förändrade kraven inom IT, kriminaltekniken och/eller polisfunktionerna.

Figur 2: Översikt av tillämpningstopologin

5.6 *Protokoll och standarder för tillämpningsarkitekturen*

5.6.1 XML

Vid utbytet av DNA-uppgifter kommer XML-schemat, som bifogas e-postmeddelanden enligt SMTP, att användas fullt ut. XML (Xtensible Markup Language) är ett av W3C rekommenderat allmänt markeringsspråk för att för särskilda ändamål skapa markeringsspråk som kan beskriva många olika former av uppgifter. En beskrivning av en DNA-profil som lämpar sig för utbyte mellan alla medlemsstater har utarbetats med hjälp av XML och XML-schemat i dokumentet för gränssnittskontroll.

5.6.2 ODBC

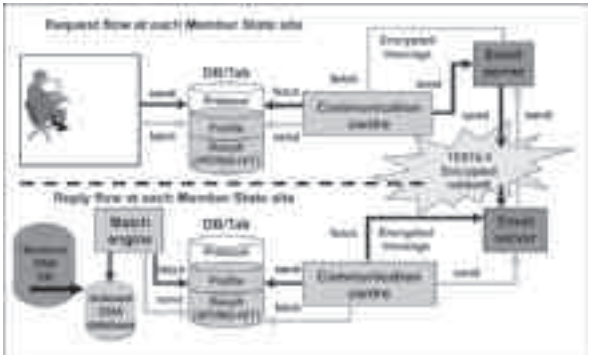
Open DataBase Connectivity tillhandahåller ett standardiserat programmeringsgränssnitt (*Application Program Interface, API*) som ger åtkomst till databashanterare, oberoende av programmeringsspråk, databassystem och operativsystem. ODBC har dock vissa nackdelar. Att hantera ett stort antal klienter kan innebära en mångfald drivrutiner och dynamiska länkbibliotek (DLL). Dessa komplikationer kan öka omkostnaderna för administration av systemet.

5.6.3 JDBC

Java DataBase Connectivity (JDBC) är ett programgränssnitt (API) for programmeringsspråket Java som definierar på vilket sätt en klient kan ha åtkomst till en databas. I motsats till *ODBC* kräver inte *JDBC* några särskilda DLL i den lokala persondatorn.

Affärslogiken för att bearbeta begäran om DNA-profiler och svar på dessa vid medlemsstaternas anläggningar beskrivs i följande diagram. Både flödet för begäran och flödet för svar växelverkar med ett neutralt dataområde bestående av olika datapooler med gemensam datastruktur.

Figur 3: Tillämpningens arbetsflöde vid medlemsstaternas anläggningar, översikt



5.7 *Kommunikationsmiljö*

5.7.1 Gemensamt kommunikationsnät: Testa och efterföljande infrastruktur

Tillämpningen för utbyte av DNA-uppgifter kommer att använda e-post, en asynkron mekanism, för att begära sökningar och ta emot svar mellan medlemsstaterna. Eftersom alla medlemsstater har minst en nationell anslutningspunkt till Testa-nätet kommer det nätet att användas för utbytet av DNA-uppgifter. Testa tillhandahåller ett antal mervärdestjänster via sitt e-postrelä. Infrastrukturen fungerar som värd för Testa-specifika e-postlådor och kan dessutom omfatta sändlistor och policy för dirigering. Detta gör att Testa kan användas som en clearingcentral för meddelanden som är adresserade till förvaltningar som är anslutna till EU-omfattande domäner. Mekanismer för viruskontroll kan också inrättas.

Relästationen för e-post i Testa är byggd på en maskinvaruplattform med hög tillgänglighet vid den centrala Testa-anläggningen och skyddas av en brandvägg. DNS-servern i Testa konverterar URL-strängar till IP-adresser så att adresseringsfrågorna inte berör användare och tillämpningar.

5.7.2 Säkerhetsfrågan

VPN-konceptet (Virtuellt Privat Nät) är genomfört inom ramen för Testa. Den teknik för *Tag Switching* som används för att bygga upp detta VPN kommer att utvecklas så att den är anpassad för den standard för *MPLS (Multi-Protocol Label Switching)* som har utarbetats av *IETF (Internet Engineering Task Force)*.

MPLS är en standardteknik från IETF som påskyndar trafikflödet i nätet genom att inte analysera paketen i mellanliggande routrar ("hops"). Detta görs med hjälp av s.k. etiketter som bifogas paketet av stamnätets gränsroutrar på grundval av information i *FIB (Forwarding Information Base)*. Etiketter används också för att genomföra virtuella privata nät.

MPLS kombinerar fördelarna med lager 3-routning och lager 2-switchning. Eftersom IP-adresserna inte analyseras vid överföringen i stamnätet, medför MPLS inte några begränsningar vad gäller IP-adresseringen.

Dessutom kommer e-postmeddelanden i Testa att skyddas av en krypteringsmekanism driven av S/MIME. Utan kännedom om nyckeln och utan rätt certifikat är det omöjligt att dekryptera meddelanden som sänds via nätet.

5.7.3 Protokoll och standarder för kommunikationsnätet

5.7.3.1 SMTP

SMTP *(Simple Mail Transfer Protocol)* är en de facto-standard för överföring av e-post via Internet. SMTP är ett relativt enkelt textbaserat protokoll där man anger en eller flera mottagare och därefter överför meddelandetexten. SMTP använder TCP-port 25 enligt IETF:s specifikation. För att hitta SMTP-servern för en visst domännamn används DNS-informationen vid MX (Mail eXchange).

Eftersom detta protokoll till att börja med uteslutande grundade sig på ASCII-text, kunde det inte hantera binära filer särskilt bra. Standarder som MIME utarbetades för att koda binära filer för överföring med SMTP. Numera är de flesta SMTP-servrarna anpassade till vidareutvecklingarna 8BITMIME och S/MIME, vilket gör att binära filer kan överföras nästan lika enkelt som klartext. Bearbetningsreglerna för S/MIME beskrivs i S/MIME-avsnittet.

SMTP är ett push-protokoll som gör att meddelanden inte kan hämtas från en fjärrserver på begäran. För att göra detta måste postkunden använda POP3 eller IMAP. Man har beslutat att använda POP3-protokollet för utbytet av DNA-uppgifter.

5.7.3.2 POP

De lokala e-postkunderna använder protokollet POP3 (*Post Office Protocol, version 3*), ett Internet-standardprotokoll för tillämpningslagret, för att hämta e-post från en fjärrserver via en TCP/IP-förbindelse. Genom att använda SMTP-protokollets profil för "skicka" sänder e-postkunder meddelanden över Internet eller över ett företagsinternt nät. MIME används som standard för bilagor och icke-ASCII-text. Även om varken POP3 eller SMTP kräver MIME-formaterad e-post, kommer så gott som all e-post via Internet i MIME-format, vilket innebär att även POP-klienterna måste förstå och använda MIME. Hela kommunikationsmiljön enligt beslut 2008/615/RIF kommer därför att inkludera POP-komponenterna.

5.7.4 Tilldelning av nätadresser

Driftsmiljö

Testa har av den europeiska IP-registreringsmyndigheten (RIPE) redan tilldelats ett särskilt block av subnet-adresser av klass C. Ytterligare block av adresser kan senare komma att tilldelas Testa vid behov. Tilldelningen av IP-adresser till medlemsstaterna grundar sig på ett geografiskt mönster i Europa. Uppgiftsutbytet mellan medlemsstaterna inom ramen för beslut 2008/615/RIF genomförs i ett logiskt slutet IP-nät som omfattar hela Europa.

Testmiljö

För att tillhandahålla en väl fungerande miljö för den dagliga verksamheten i alla anslutna medlemsstater måste en testmiljö upprättas i det slutna nätet för nya medlemsstater som förbereder sitt deltagande. Ett blad med parametrar, bland annat IP-adresser, nätinställningar, e-postdomäner och användarkonton för tillämpningen har utarbetats och bör anslås vid dessa medlemsstaters anläggningar. En uppsättning pseudo-DNA-profiler för teständamål har också utformats.

5.7.5 Konfigurationsparametrar

Ett säkert e-postsystem har upprättats med användning av domänen eu-admin.net. Denna domän kommer inte att kunna nås från en plats som inte ingår i den EU-omfattande Testa-domänen, eftersom namnen endast är kända på Testas centrala DNS-server, som är skyddad från Internet.

Mappningen av dessa webbplatsadresser (värdnamn) till motsvarande IP-adresser sköts genom DNS-tjänsten i Testa. För varje lokal domän kommer ett postobjekt att läggas till på Testas centrala DNS-server, varifrån alla e-postmeddelanden från Testas lokala domäner skickas vidare till Testas centrala postrelä. Det centrala postrelät kommer därefter att vidarebefordra dem till den specifika lokala domänens e-postserver och använda de lokala domänernas e-postadresser. Genom att skicka vidare e-posten på detta sätt kommer kritisk information i e-postmeddelandena endast att passera den EU-omfattande slutna nätinfrastrukturen, inte det osäkra Internet.

Subdomäner (***fet kursiv stil***) enligt följande syntax måste upprättas för alla medlemsstaters anläggningar:

"***typ_av_tillämpning*.pruem.*medlemsstatskod.eu-admin*.*net***", där

värdet för "***medlemsstatskod***" är en av de tvåställiga bokstavskoderna för medlemsstaterna (dvs. "AT", "BE" etc.), och

värdet för "***typ_av_tillämpning***" är antingen DNA eller FP.

Med denna syntax blir medlemsstaternas subdomäner följande:

MS	Sub Domains	Comments
BE	***dna*.pruem.be**.eu-admin.net	Setting up a secure local link to the existing TESTA II access point
	***fp*.pruem.be**.eu-admin.net	
BG	***dna*.pruem.bg**.eu-admin.net	
	***fp*.pruem.bg**.eu-admin.net	
CZ	***dna*.pruem.cz**.eu-admin.net	
	***fp*.pruem.cz**.eu-admin.net	
DK	***dna*.pruem.dk**.eu-admin.net	
	***fp*.pruem.dk**.eu-admin.net	
DE	***dna*.pruem.de**.eu-admin.net	Using the existing TESTA II national access points
	***fp*.pruem.de**.eu-admin.net	
EE	***dna*.pruem.ee**.eu-admin.net	
	***fp*.pruem.ee**.eu-admin.net	

MS	Sub Domains	Comments
IE	***dna*.pruem.ie**.eu-admin.net	
	***fp*.pruem.ie**.eu-admin.net	
EL	***dna*.pruem.el**.eu-admin.net	
	***fp*.pruem.el**.eu-admin.net	
ES	***dna*.pruem.es**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.es**.eu-admin.net	
FR	***dna*.pruem.fr**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.fr**.eu-admin.net	
IT	***dna*.pruem.it**.eu-admin.net	
	***fp*.pruem.it**.eu-admin.net	
CY	***dna*.pruem.cy**.eu-admin.net	
	***fp*.pruem.cy**.eu-admin.net	
LV	***dna*.pruem.lv**.eu-admin.net	
	***fp*.pruem.lv**.eu-admin.net	
LT	***dna*.pruem.lt**.eu-admin.net	
	***fp*.pruem.lt**.eu-admin.net	
LU	***dna*.pruem.lu**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.lu**.eu-admin.net	
HU	***dna*.pruem.hu**.eu-admin.net	
	***fp*.pruem.hu**.eu-admin.net	
MT	***dna*.pruem.mt**.eu-admin.net	
	***fp*.pruem.mt**.eu-admin.net	
NL	***dna*.pruem.nl**.eu-admin.net	Intending to establish a new TESTA II access point at the NFI
	***fp*.pruem.nl**.eu-admin.net	
AT	***dna*.pruem.at**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.at**.eu-admin.net	
PL	***dna*.pruem.pl**.eu-admin.net	
	***fp*.pruem.pl**.eu-admin.net	
PT	***dna*.pruem.pt**.eu-admin.net	...
	***fp*.pruem.pt**.eu-admin.net	...
RO	***dna*.pruem.ro**.eu-admin.net	
	***fp*.pruem.ro**.eu-admin.net	

MS	Sub Domains	Comments
SI	***dna*.pruem.si**.eu-admin.net	...
	***fp*.pruem.si**.eu-admin.net	...
SK	***dna*.pruem.sk**.eu-admin.net	
	***fp*.pruem.sk**.eu-admin.net	
FI	***dna*.pruem.fi**.eu-admin.net	*[To be inserted]*
	***fp*.pruem.fi**.eu-admin.net	
SE	***dna*.pruem.se**.eu-admin.net	
	***fp*.pruem.se**.eu-admin.net	
UK	***dna*.pruem.uk**.eu-admin.net	
	***fp*.pruem.uk**.eu-admin.net	

KAPITEL 2: **Utbyte av fingeravtrycksuppgifter (gränssnittskontrolldokument)**

Syftet med följande gränssnittskontrolldokument är att fastställa kraven för utbytet av fingeravtrycksuppgifter mellan AFIS-systemen i medlemsstaterna (Automated Fingerprint Identification Systems). Det grundar sig på Interpols implementation av ANSI/NIST-ITL 1-2000 (INT-I, version 4.22b).

Denna version ska omfatta alla grundläggande definitioner för de logiska posterna av typ 1, typ 2, typ 4, typ 9, typ 13 och typ 15 som krävs för bearbetning av fingeravtrycken utgående från bilder och minutiae.

1. ***Översikt av filinnehållet***

En fingeravtrycksfil består av flera logiska poster. I den ursprungliga standarden ANSI/NIST-ITL 1-2000 specificeras 16 posttyper. Lämpliga ASCII-avgränsare sätts in mellan posterna och mellan fält och delfält i posterna.

Endast sex posttyper används för att utbyta uppgifter mellan det sändande och det mottagande organet.

Typ 1 → Transaktionsinformation

Typ 2 → Alfanumeriska person- och/eller ärendeuppgifter

Typ 4 → Högupplösta fingeravtrycksbilder i gråskala

Typ 9 → Minutiaepost

Typ 13 → Post för latent bild med varierande upplösning

Typ 15 → Post för handavtrycksbild med varierande upplösning

1.1 *Typ 1 – Filhuvud*

Denna post innehåller routningsinformation och information som beskriver strukturen i resten av filen. Denna posttyp definierar också transaktionstypen, som ingår i någon av följande övergripande kategorier:

1.2 *Typ 2 – Beskrivande text*

Denna post innehåller informerande text av intresse för det sändande och det mottagande organet.

1.3 *Typ 4 – Högupplöst bild i gråskala*

Denna post används för att utbyta högupplösta fingeravtrycksbilder i gråskala (8 bitar) som skannats med upplösningen 500 pixel/tum. Fingeravtrycksbilderna ska komprimeras med WSQ-algoritmen i ett förhållande som inte överstiger 15:1. Andra komprimeringsalgoritmer eller okomprimerade bilder får inte användas.

1.4 *Typ 9 – Minutiaepost*

Posttyp 9 används för att utbyta karakteristiska papillarmönster eller uppgifter om minutiae. De tjänar dels till undvika onödig dubblering av AFIS-kodningsprocesserna, dels till att göra det möjligt att överföra AFIS-koder som innehåller färre uppgifter än motsvarande bilder.

1.5 *Typ 13 – Latenta bilder med varierande upplösning*

Denna post ska användas för att utbyta bilder av latenta fingeravtryck och handavtryck tillsammans med alfanumerisk textinformation. Bilder ska vara skannade med upplösningen 500 pixel/tum i 256 nivåer av grått. Om den latenta bildens kvalitet tillåter det, ska den komprimeras med WSQ-algoritmen. Om så behövs får, efter ömsesidig överenskommelse, bildernas upplösning ökas så att den överskrider 500 pixel/tum och gråskalan utvidgas till fler än 256 nivåer. I detta fall bör man absolut använda JPEG 2000 (se bilaga 7).

1.6 *Post för handavtrycksbild med varierande upplösning*

Poster av typ 15 med taggade fält ska användas för att utbyta handavtrycksbilder med varierande upplösning tillsammans med alfanumerisk textinformation. Bilder ska vara skannade med upplösningen 500 pixel/tum i 256 nivåer av grått. För att minimera datamängderna ska alla handavtrycksbilder komprimeras med WSQ-mekanismen. Om så behövs får, efter ömsesidig överenskommelse, bildernas upplösning ökas så att den överskrider 500 pixel/tum och gråskalan utvidgas till fler än 256 nivåer. I detta fall bör man absolut använda JPEG 2000 (se bilaga 7).

2. ***Postformat***

En transaktionsfil ska bestå av en eller flera logiska poster. I varje logisk post i filen ska det finnas flera fält med information associerad med posttypen i fråga. Varje informationsfält kan innehålla en eller flera grundläggande uppgifter som var och en representeras av endast ett värde. Sammantagna används dessa uppgifter för att förmedla olika aspekter av informationen i fältet. Ett informationsfält kan också bestå av en eller flera grupperade uppgifter som upprepas flera gånger inom fältet. En sådan grupp av uppgifter kallas delfält. Ett informationsfält kan därför bestå av ett eller delfält med uppgifter.

2.1 *Informationsavgränsare*

I de logiska posterna med taggade fält skiljs de olika informationskomponenterna från varandra med hjälp av fyra informationsavgränsare i ASCII-kod. De på så sätt avgränsade informationskomponenterna kan vara uppgifter inom ett fält eller ett delfält, fält i en logisk post eller de olika förekomsterna av delfält. Dessa informationsavgränsare definieras i ANSI X3.4-standarden. Dessa tecken används för att avgränsa och kvalificera information i logisk mening. Sedda i hierarkisk ordning uppifrån och ner är filavgränsningstecknet "FS" den mest inklusiva avgränsaren, följd av gruppavgränsaren "GS", postavgränsaren "RS" och sist enhetsavgränsningstecknet "US". Dessa ASCII-avgränsare, och hur de används inom ramen för denna standard, beskrivs i tabell 1.

Informationsavgränsarna bör ur funktionell synpunkt ses som en anvisning om vilken typ av information som följer efter avgränsaren. US-tecknet ska avgränsa olika enskilda uppgifter inom ett fält eller ett delfält. Det är en signal om att nästa uppgift är en informationskomponent inom det fältet eller delfältet. Flera olika delfält inom ett fält avgränsade med RS-tecknet signalerar början av nästa grupp av upprepade uppgifter. Avgränsningstecknet GS mellan informationsfält signalerar början av ett nytt fält och ska föregå det fältidentifikationsnummer som ska finnas. På liknande sätt ska början av en ny logisk post signaleras av FS-tecknet.

De fyra tecknen är endast meningsfulla när de används som avgränsare av informationskomponenter i fält i poster med ASCII-text. Dessa tecken har ingen särskild betydelse när de förekommer i binära bildposter och binära fält – de ingår då endast i de utbytta uppgifterna.

Det ska normalt inte finnas tomma fält eller uppgifter, och därför bör det endast förekomma ett avgränsningstecken mellan två uppgifter. Undantaget från denna regel inträffar till exempel när data i ett fält eller uppgifter i en transaktion inte är tillgängliga, saknas eller är frivilliga, och bearbetningen av transaktionen inte är beroende av att dessa specifika data finns att tillgå. I dessa fall ska flera och angränsande avgränsningstecken förekomma tillsammans, snarare än att uppgifter utan betydelse infogas mellan avgränsningstecknen.

Följande gäller för definitionen av ett fält som består av tre uppgifter. Om information för den andra uppgiften saknas, kommer två angränsande US-avgränsare att förekomma mellan den första och den tredje uppgiften. Om både den andra och den tredje uppgiften saknades, skulle tre avgränsningstecken användas – två US-tecken förutom den avslutande fält- eller delfältsavgränsaren. Allmänt sett gäller att om en eller flera obligatoriska eller frivilliga uppgifter inte finns att tillgå för ett fält eller ett delfält, ska det relevanta antalet avgränsningstecken infogas.

Det är möjligt att ha kombinationer med två eller flera av de fyra tillgängliga avgränsningstecknen gränsande till varandra. Om data saknas eller inte finns att tillgå för uppgifter, delfält eller fält, måste det förekomma ett avgränsningstecken mindre än antalet erforderliga uppgifter, delfält eller fält.

Tabell 1: Använda avgränsare

Code	Type	Description	Hexadecimal Value	Decimal Value
US	Unit Separator	Separates information items	1F	31
RS	Record Separator	Separates subfields	1E	30
GS	Group Separator	Separates fields	1D	29
FS	File Separator	Separates logical records	1C	28

2.2 *Postformat*

I logiska poster med taggade fält ska varje informationsfält som används numreras i enlighet med följande standard. Varje fält ska formateras så att det består av typnummer för den logiska posten följt av punkt ".", ett fältnummer följt av kolon ":", följt av den för detta fält relevanta informationen. Fältnumret för det taggade fältet kan vara ett godtyckligt en- till niosiffrigt nummer som förekommer mellan punkt "." och kolon ":". Det ska tolkas som ett fältnummer i positivt heltal. Detta innebär att ett fältnummer "2 123:" är lika med och ska tolkas på samma sätt som ett fältnummer "2.000000123:".

I exemplifierande syfte används i hela detta dokument ett treställigt tal för numrering av de fält som ingår de logiska poster med taggade fält som beskrivs i dokumentet. Fältnummer får formatet "TT.xxx:" där "TT" representerar posttypen med ett eller två tecken följt av en punkt. De följande tre tecknen innehåller det relevanta fältnumret som följs av ett kolon. Efter kolon följer ASCII-information eller bilddata.

Logiska poster av typ 1 eller typ 2 innehåller endast datafält med ASCII-text. Den totala postlängden (inklusive fältnummer, kolon och avgränsningstecken) ska anges i det första ASCII-fältet i båda dessa posttyper. ASCII-filavgränsaren "FS" (anger slutet av den logiska posten eller transaktionen) ska följa efter den sista positionen ASCII-information och inkluderas i postlängden.

I motsats till konceptet med taggade fält innehåller poster av typ 4 endast binära data som registrerats i form av ordnade binära fält med fast längd. Den totala postlängden ska anges i det första fältet om fyra positioner i varje post. I denna binära post ska varken postnumret med sin efterföljande punkt eller fältnumret med efterföljande kolon anges. Eftersom alla fältlängder i denna posttyp antingen är fasta eller specificerade, ska inget av de fyra avgränsningstecknen ("US", "RS", "GS", eller "FS") tolkas som någonting annat än binära data. FS-tecknet ska inte användas som post- eller transaktionsavgränsare i den binära posten.

3. ***Logisk post typ 1: Filhuvud***

Denna post beskriver filens struktur och typ samt innehåller annan viktig information. De tecken som används för fält i logiska poster av typ 1 ska endast utgöras av den 7-bitars ANSI-koden för informationsutbyte.

3.1 *Fält i logisk post typ 1*

3.1.1 Fält 1.001: Logisk postlängd (*Logical Record Length – LEN*)

I detta fält anges det totala antalet byte i hela den logiska posten av typ 1. Fältet inleds med "1 001:" följt av den totala postlängden, inklusive alla tecken i alla fält och informationsavgränsarna.

3.1.2 Fält 1.002: Versionsnummer (*Version number – VER*)

För att säkerställa att användarna känner till vilken version av ANSI/NIST-standarden som används, anges i detta fält versionsnumret för den standard som används av det program eller system som har skapat filen. I de första två positionerna anges versionsnumret, i de två följande revisionsnumret. Den ursprungliga standarden från 1986 skulle till exempel anses som den första versionen och anges som "0100", medan den nuvarande standarden ANSI/NIST-ITL 1-2000 anges som "0300".

3.1.3 Fält 1.002: Fältinnehåll (File Content – CNT)

I detta fält förtecknas varje post i filen efter posttyp och i den ordning i vilken de förekommer i den logiska filen. Det består av ett eller flera delfält, som vart och ett i sin tur innehåller två uppgifter som beskriver en logisk post som förekommer i den aktuella filen. Delfälten registreras i samma ordning som den i vilken posterna registreras och överförs.

Den första uppgiften i det första delfältet är "1", vilket hänvisar till denna post av typ 1. Den följs av en andra uppgift om antalet andra poster som förekommer i filen. Detta antal är också lika med antal återstående delfält i fält 1.003.

Vart och ett av de återstående delfälten är förknippat med en post i filen och sekvensen av delfält svarar mot sekvensen av poster. Varje delfält innehåller två uppgifter. Den första uppgiften identifierar posttypen. Den andra uppgiften är postens IDC. US-tecknet ska användas för att avgränsa de två uppgifterna.

3.1.4 Fält 1.003: Transaktionstyp (*Type of Transaction – TOT*)

Detta fält innehåller en treställig minneskod som anger transaktionstypen. Dessa koder kan skilja sig från dem som används i andra implementationer av ANSI/NIST-standarden.

CPS: Criminal Print-to-Print Search. Transaktionen är en begäran om sökning med en post i anslutning till ett brott mot en avtrycksdatabas. Personens avtryck måste inkluderas i filen som WSQ-komprimerade bilder.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1–14 poster typ 4.

Transaktionstypen CPS sammanfattas i tabell A.6.1 (bilaga 6).

PMS: Print-to-Latent Search. Denna transaktion används när en uppsättning avtryck ska användas för sökning mot en databas med oidentifierade latenta avtryck. Svaret kommer att innehålla Träff/Icke-träff-avgörandet vid den avsedda AFIS-sökningen. Om det finns flera oidentifierade latenta avtryck, kommer flera SRE-transaktioner att returneras med ett latent avtryck per transaktion. Personens avtryck måste inkluderas i filen som WSQ-komprimerade bilder.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1 post typ 13.

Transaktionstypen PMS sammanfattas i tabell A.6.1 (bilaga 6).

MPS: Latent-to-Print Search. Denna transaktion används när ett latent avtryck ska användas för sökning mot en avtrycksdatabas. Den latenta minutiaeinformationen och bilden (WSQ-komprimerad) måste ingå i filen.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1 post typ 4 eller typ 15.

Transaktionstypen MPS sammanfattas i tabell A.6.4 (bilaga 6).

MMS: Latent-to-Latent Search. För denna transaktion innehåller filen ett latent avtryck som ska användas för sökning mot en databas med oidentifierade latenta avtryck i syfte att ta konstatera kopplingar mellan olika brottsplatser. Den latenta minutiaeinformationen och bilden (WSQ-komprimerad) måste ingå i filen.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1 post typ 13.

Transaktionstypen MMS sammanfattas i tabell A.6.4 (bilaga 6).

SRE: Denna transaktion returneras av bestämmelseorganet som svar på begäran om fingeravtrycksundersökningar. Svaret kommer att innehålla Träff/Icke-träff-avgörandet vid den avsedda AFIS-sökningen. Om det finns flera kandidater, kommer flera SRE-transaktioner att returneras med en kandidat per transaktion.

Transaktionstypen SRE sammanfattas i tabell A.6.2 (bilaga 6).

ERR: Denna transaktion returneras av det avsedda AFIS-systemet för att ange ett fel vid bearbetningen av transaktionen. Den innehåller ett meddelandefält (ERM) som anger vilket fel som har upptäckts. Följande logiska poster kommer att returneras:

— 1 post typ 1.

— 1 post typ 2.

Transaktionstypen ERR sammanfattas i tabell A.6.3 (bilaga 6).

Tabell 2: Tillåtna koder i transaktioner

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
CPS	M	M	M	—	—	—
SRE	M	M	C	— (C in case of latent hits)	C	C
MPS	M	M	—	M (1*)	M	—

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
MMS	M	M	—	M (1*)	M	—
PMS	M	M	M*	—	—	M*
ERR	M	M	—	—	—	—

Nyckel:

M = Obligatorisk
M* = Endast en av båda posttyperna får ingå
O = Frivillig
C = Beroende av tillgängliga uppgifter
– = Ej tillåten
1* = Beroende av legacy systems

3.1.5 Fält 1.005: Transaktionsdatum (*Date of Transaction – DAT*)

Detta fält anger vilken dag transaktionen initierades och måste följa ISO-standarden YYYYMMDD

där YYYY är året, MM är månaden och DD är dagen i månaden. Ledande nollor ska användas för ensiffriga tal. "19931004" står till exempel för den 4 oktober 1993.

3.1.6 Fält 1.006: PRIORITET (*Priority – PRY*)

Detta frivilliga fält anger prioritet, på en nivå 1–9, för begäran. "1" anger högsta prioritet, "9" lägsta prioritet. Prioritet "1" ska behandlas omedelbart.

3.1.7 Fält 1.007: Bestämmelseorgansidentifierare (Destination Agency Identifier – DAI)

Detta fält anger transaktionens bestämmelseorgan.

Det består av två uppgifter i följande format: CC/*organ*.

Den första uppgiften består av en landskod om två alfanumeriska tecken enligt ISO 3166. Den andra uppgiften, *organ*, identifierar organet genom en sträng fri text om maximalt 32 alfanumeriska tecken.

3.1.8 Fält 1.008: Ursprungsorgansidentifierare (*Originating Agency Identifier – ORI*)

Detta fält anger vilket organ som har skapat filen och har samma format som DAI (fält 1.007).

3.1.9 Fält 1.009: Transaktionskontrollnummer (*Transaction Control Number – TCN*)

Detta är ett kontrollnummer för hänvisningsändamål. Det bör skapas av datorn och ha följande format: YYSSSSSSSSA

där YY är år för transaktionen, SSSSSSSS är ett åttaställligt serienummer och A är ett kontrolltecken som har genererats med den procedur som anges i bilaga 2.

Om TCN inte är tillgängligt, ska fältet YYSSSSSSSS fyllas med nollor och det kontrolltecken som genererats enligt ovan.

3.1.10 Fält 1.010: Transaktionskontrollsvar (Transaction Control Response – TCR)

När en begäran har sänts med denna post som svar, innehåller detta frivilliga fält Transaction Control Number (TCN) för meddelandet med begäran. Det har därför samma format som TCN (fält 1.009).

3.1.11 Fält 1.011: (Native Scanning Resolution – NSR)

Detta fält anger den normala upplösningen vid skanning för det system som avsändaren av transaktionen använder. Upplösningen ska anges med två siffror följd av decimalpunkt och därefter ytterligare två siffror.

För alla transaktioner i enlighet med beslut 2008/615/RIF ska samplingsfrekvensen vara 500 pixel/tum eller 19,68 pixel/mm.

3.1.12 Fält 1.012: Nominell överföringsresolution (Nominal Transmitting Resolution – NTR)

Detta fält om fem positioner anger nominell överföringsupplösning för de bilder som överförs. Upplösningen ska uttryckas i pixel/mm i samma format som NSR (fält 1.011).

3.1.13 Fält 1.013: Domännamn (Domaine Name – DOM)

I detta obligatoriska fält anges domännamnet för den användardefinierade implementationen av logisk post typ 2. Det innehåller två uppgifter och ska uttryckas som "INT-I{US}4.22{GS}".

3.1.14 Fält 1.014: Greenwich Mean Time (GMT)

Detta obligatoriska fält ger möjlighet att uttrycka datum och tidpunkt i GMT-enheter (Greenwich Mean Time). Om det används innehåller GMT-fältet universellt datum i tillägg till det lokala datum som anges i fält 1.005 (DAT). Om GMT-fältet används elimineras inkonsekvenser med lokal tid när en transaktion och dess svar överförs mellan två platser skilda åt av flera tidszoner. GMT ger ett universellt datum och en 24-timmarstid som är oberoende av tidszoner. Fältet anges som "CCYYMMDDHHMMSSZ", en 15-positioners teckensträng som utgörs av datum konkatenerat med GMT och avslutas med "Z". Tecknen "CCYY" ska representera år för transaktionen, tecknen "MM" ska ange tiotals- och entalssiffran för månad, tecknen "DD" ska ange tiotals- och entalssiffran för dag i månaden, tecknen "HH" ska ange timme, "MM" ska ange minut och "SS" ska ange sekund. Den fullständiga tidsangivelsen får inte ange en tidpunkt i framtiden.

4. ***Logisk post typ 2: Beskrivande text***

Större delen av denna posts struktur definieras inte genom den ursprungliga ANSI/NIST-standarden. Posten innehåller information av särskilt intresse för de organ som sänder eller tar emot filen. För att säkerställa att de kommunicerande fingeravtryckssystemen är kompatibla kräver detta ICD att posten innehåller endast de fält som förtecknas nedan. I dokumentet anges vilka fält som är obligatoriska frivilliga, samtidigt som de enskilda fältens struktur fastställs.

4.1 *Fält i logisk post typ 2*

4.1.1 Fält 2.001: Logisk postlängd (*Logical Record Length – LEN*)

Detta obligatoriska fält anger längden av typ 2-posten i totalt antal byte, inklusive varje tecken i varje fält och informationsavgränsarna.

4.1.2 Fält 2.002: *Bilddesigneringstecken* (IDC)

Den IDC som anges i detta obligatoriska fält är en ASCII-representation av den IDC som definieras i fältet File Content i typ 1-posten.

4.1.3 Fält 2.003: Systeminformation (*System Information – SYS*)

Detta fält om fyra positioner är obligatoriskt och anger vilken version av INT-I som just denna typ 2-post följer.

I de första två positionerna anges versionsnumret, i de två följande revisionsnumret. Denna implementation grundar sig till exempel på INT-I version 2 revision 22, vilket ska uttryckas som "0422".

4.1.4 Fält 2.007: Ärendenummer (*Case Number – CNO*)

Detta är ett nummer som av det lokala fingeravtrycksorganet tilldelas en samling latenta avtryck som hittas på brottsplatsen. Följande format ska användas: CC/*nummer*

där "CC" är Interpols landskod med två alfanumeriska tecken och *nummer* följer de relevanta lokala riktlinjerna och kan bestå av upp till 32 alfanumeriska tecken.

Genom detta fält kan systemet identifiera latenta avtryck förknippade med ett visst brott.

4.1.5 Fält 2.008: Sekvensnummer (Sequence Number – SQN)

Detta specificerar varje sekvens av latenta avtryck inom ett fall. Det kan innehålla upp till fyra numeriska tecken. En sekvens är ett latent avtryck eller serier av latenta avtryck som förs samman i grupper för registrering och/eller sökning. Denna definition medför att även enskilda latenta avtryck måste tilldelas ett sekvensnummer.

Detta fält kan tillsammans med MID (fält 2.009) användas för att identifiera ett särskilt latent avtryck i sekvensen.

4.1.6 Fält 2.009: Latentavtrycksidentifierare (Latent Identifier – MID)

Detta fält specificerar det enskilda latenta avtrycket inom en sekvens. Värdet är en eller två bokstäver där "A" tilldelas det första latenta avtrycket, "B" tilldelas det andra och så vidare upp till gränsen "ZZ". Fältet används på samma sätt som sekvensnumret för det latenta avtrycket enligt beskrivningen av SQN (fält 2.008).

4.1.7 Fält 2.010: Brottsreferensnummer (Criminal Reference Number – CRN)

Detta är ett unikt referensnummer som ett nationellt organ tilldelar en person när denna för första gången döms för att ha begått ett brott. I ett visst land har en person aldrig mer än ett CRN, eller delar det med en annan person. Samma person kan emellertid ha Criminal Reference Numbers i flera länder, dessa kan då skiljas åt med hjälp av landskoden.

CRN-fältet ska ha följande format: CC/nummer

där "CC" är landskod med två alfanumeriska tecken enligt ISO 3166 och *nummer* följer relevanta nationella riktlinjer från det utfärdande organet och kan bestå av upp till 32 alfanumeriska tecken.

I transaktioner i enlighet med beslut 2008/615/RIF kommer detta fält att användas för nationellt Criminal Reference Number från det organ som är kopplat till bilderna i poster av typ 4 eller typ 15.

4.1.8 Fält 2.012: (*Miscellaneous Identification Number – MN1*)

Detta fält innehåller det CRN (fält 2.010) som sänts med en CPS- eller PMS-transaktion, utan inledande landskod.

4.1.9 Fält 2.013: (*Miscellaneous Identification Number – MN2*)

Detta fält innehåller det CRO (fält 2.007) som sänts med en MPS- eller MMS-transaktion, utan inledande landskod.

4.1.10 Fält 2.014: (*Miscellaneous Identification Number – MN3*)

Detta fält innehåller det SQN (fält 2.008) som sänts med en MPS- eller MMS-transaktion.

4.1.11 Fält 2.015: (*Miscellaneous Identification Number – MN4*)

Detta fält innehåller det SQN (fält 2.009) som sänts med en MPS- eller MMS-transaktion.

4.1.12 Fält 2.063: Tilläggsinformation (*Additional Information – INF*)

Vid en SRE-transaktion efter en PMS-begäran informerar detta fält om vilket finger som gav anledning till den eventuella träffen. Fältet ska ha följande format:

NN där *NN* är den tvåställiga fingerpositionskod som definieras i tabell 5.

I alla övriga fall är detta fält frivilligt. Det består av upp till 32 alfanumeriska tecken och kan användas för att lämna ytterligare upplysningar om begäran.

4.1.13 Fält 2.064: (*Respondents List – RLS*)

Detta fält innehåller minst två delfält. Det första delfältet beskriver den typ av sökning som har gjorts med användning av den treställiga minneskod som specificerar transaktionstypen i TOT-fältet (fält 1.004). Det andra delfältet består av endast ett tecken. "I" ska användas för att ange en TRÄFF, och "N" ska användas för att ange att inga överensstämmelser har hittats (ICKE-TRÄFF). Det tredje delfältet innehåller sekvensidentifieraren för kandidatresultatet och totalt antal kandidater, avgränsat med snedstreck. Flera meddelanden kommer att returneras om det finns fler än en kandidat.

Vid en eventuell TRÄFF ska fjärde delfältet innehålla träffvärdet med upp till tio siffror. Om TRÄFFen har verifierats ska värdet för detta delfält definieras som "999999".

Exempel: "CPS{RS}I{RS}001/001{RS}999999{GS}"

Om det AFIS till vilket transaktionen sänds inte tilldelar träffvärden, ska träffvärdet noll föras in på rätt plats.

4.1.14 Fält 2.074: Fält för status- och felmeddelanden (*Status/Error Message Field – ERM*)

Detta fält innehåller felmeddelanden vid transaktionsbearbetningen, vilka sänds tillbaka till den begärande parten som del av en feltransaktion.

Tabell 3: Felmeddelanden

Numeric Code (1-3)	Meaning (5-128)
003	ERROR: UNAUTHORISED ACCESS
101	Mandatory field missing
102	Invalid record type
103	Undefined field
104	Exceed the maximum occurrence
105	Invalid number of subfields
106	Field length too short
107	Field length too long
108	Field is not a number as expected
109	Field number value too small
110	Field number value too big
111	Invalid character
112	Invalid date
115	Invalid item value
116	Invalid type of transaction
117	Invalid record data
201	ERROR: INVALID TCN
501	ERROR: INSUFFICIENT FINGERPRINT QUALITY
502	ERROR: MISSING FINGERPRINTS
503	ERROR: FINGERPRINT SEQUENCE CHECK FAILED
999	ERROR: ANY OTHER ERROR. FOR FURTHER DETAILS CALL DESTINATION AGENCY.

Felmeddelanden i intervallet 100–199:

Dessa felmeddelanden gäller kontrollen av ANSI/NIST-posterna och ska uttryckas som

<error_code 1>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

<error_code 2>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

där

— error_code är en kod som är entydigt kopplad till en viss orsak (se tabell 3),

— field_id är ANSI/NIST-fältnumret för det felaktiga fältet (t.ex. 1.001, 2.001, ...) i formatet <record_type>.<field_id>.<sub_field_id>,

— dynamic text är en mer utförlig situationsanpassad beskrivning av felet,

— LF är ett LF-tecken som avgränsar felen om fler än ett fel har påträffats,

— för typ 1-poster fastställs ICD till "-1".

Exempel:

201: IDC - 1 FIELD 1 009 FEL KONTROLLTECKEN {LF} 115: IDC 0 FIELD 2 003 OGILTIG SYSTEMINFORMATION

Detta fält är obligatoriskt för feltransaktioner.

4.1.15 Fält 2.320: Förväntat antal kandidater (*Expected Number of Candidates – ENC*)

Detta fält anger det maximala antal kandidater för kontroll som det begärande organet förväntar sig. Värdet ENC får inte överskrida de värden som definieras i tabell 11.

5. ***Logisk post typ 4: Högupplösningsbild i gråskala***

Det bör noteras att poster av typ 4 är binära poster snarare än ASCII-poster. Varje fält har där tilldelats en specifik position i posten, vilket medför att alla fält är obligatoriska.

Standarden medger att både bildstorlek och upplösning anges i posten. Logisk posttyp 4 måste innehålla fingeravtrycksuppgifter som överförs med en nominell pixeltäthet av 500–520 pixel/tum. Den täthet som föredras för nyutformningar är 500 pixel per tum, dvs. 19,68 pixel per mm. 500 pixel per tum är den täthet som specificeras i INT-I, med undantag för att liknande system får kommunicera med användning av en annan täthet inom intervallet 500–520 pixel per tum.

5.1 *Fält i logisk post typ 4*

5.1.1 Fält 4.001: Logisk postlängd (*Logical Record Length – LEN*)

Detta fält om fyra byte anger längden av typ 4-posten i totalt antal byte, inklusive varje byte i varje fält.

5.1.2 Fält 4.002: Bilddesigneringstecken (*Image Designation Character – IDC*)

Detta fält innehåller i binär form IDC-numret i filhuvudet.

5.1.3 Fält 4.003: Avtryckstyp (*Impression Type – IMP*)

Avtryckstyp är ett fält om en byte i sjätte positionen i posten.

Tabell 4: Fingeravtryckstyp

	Description
0	Live-scan of plain fingerprint
1	Live-scan of rolled fingerprint
2	Non-live scan impression of plain fingerprint captured from paper
3	Non-live scan impression of rolled fingerprint captured from paper
4	Latent impression captured directly
5	Latent tracing

	Description
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4 Fält 4.004: Fingerposition (Finger Position – FGP)

Detta fasta fält med 6 byte upptar positionerna 7–12 i en post av typ 4. Det innehåller möjliga fingerställningar med början i den byte som befinner sig längst till vänster (byte 7 i posten). Känd eller mest trolig fingerposition har tagits från tabell 5. Upp till fem ytterligare fingrar kan registreras genom att man lägger in alternerande fingerpositioner i återstående fem byte i samma format. Om färre än fem fingerpositionsreferenser används fylls oanvända byte med binära 255. För att registrera alla fingerpositioner används 0 för okänd.

Tabell 5: Fingerposition och maximal storlek

Finger position	Finger code	Width (mm)	Length (mm)
Unknown	0	40,0	40,0
Right thumb	1	45,0	40,0
Right index finger	2	40,0	40,0
Right middle finger	3	40,0	40,0
Right ring finger	4	40,0	40,0
Right little finger	5	33,0	40,0
Left thumb	6	45,0	40,0
Left index finger	7	40,0	40,0
Left middle finger	8	40,0	40,0
Left ring finger	9	40,0	40,0
Left little finger	10	33,0	40,0
Plain right thumb	11	30,0	55,0
Plain left thumb	12	30,0	55,0
Plain right four fingers	13	70,0	65,0
Plain left four fingers	14	70,0	65,0

För latenta fingeravtryck på brottsplatsen bör endast koderna 0-10 användas.

5.1.5 Fält 4.005: Bildskanningsupplösning (*Image Scanning Resolution – ISR*)

Detta fält om en byte upptar position 13 i typ 4-posten. Om det innehåller "0" har bilden skannats med en föredragen upplösning på 19,68 pixel/mm (500 pixel per tum). Om det innehåller "1" har bilden skannats med en alternativ upplösning enligt typ 1-posten.

5.1.6 Fält 4.006: Horisontell linjelängd (*Horizontal Line Length – HLL*)

I detta fält som upptar positionerna 14-15 i typ 4-posten anges antalet pixel i varje skanningslinje. Den första positionen är mest signifikant.

5.1.7 Fält 4.007: Vertikal linjelängd (*Vertical Line Length – VLL*)

I detta fält i positionerna 16–17 anges antalet skanningslinjer i bilden. Den första positionen är mest signifikant.

5.1.8 Fält 4.008: Algoritm för komprimering av gråskalan (*Gray-scale Compression Algorithm – GCA*)

I detta fält om en byte anges vilken algoritm för komprimering av gråskalan som har använts för att koda bilddata. En binär kod 1 anger att WSQ-komprimering (bilaga 7 har använts för denna implementation.

5.1.9 Fält 4.009: Bilden (*The Image*)

Detta fält innehåller en teckensträng som representerar bilden. Fältets struktur kommer uppenbarligen att vara beroende av vilken komprimeringsalgoritm som används.

6. ***Logisk post typ 9: Minutiaepost***

Typ 9-poster ska innehålla ASCII-text som beskriver minutiae och dithörande uppgifter som har registrerats från ett latent avtryck. För en sökning efter latenta avtryck finns ingen övre gräns för antalet typ 9-poster i filen, som var och en ska svara mot en annan vy eller latent avtryck.

6.1 *Extraktion av minutiae*

6.1.1 Identifiering av minutiaetypen

I denna standard definieras tre identifikationsnummer som används för att beskriva minutiaetypen. Dessa specifikationer förtecknas i tabell 6. Åsavslutningar ska betecknas typ 1. Förgreningar ska betecknas typ 2. Om en minutiae inte klart kan kategoriseras en av de ovan nämnda typerna ska den betecknas som "annan", typ 0.

Tabell 6: Minutiaetyper

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2 Typ och placering av minutiae

För att mallarna ska uppfylla kraven i avsnitt 5 i standarden ANSI INCITS 378-2004, ska följande metod, som förstärker den nu gällande standarden INCITS 378-20204, användas för att bestämma placering (läge och vinkelriktning) för enskilda minutiae.

Positionen eller läget för en minutia som representerar avslutningen på en ås ska vara gaffelpunkten i dalområdets mittskelett omedelbart framför åsavslutningen. Om de tre benen i dalområdet tunnas ner till en skelettbild som är en enda pixel bred, är det skärningspunkten som är minutians läge. På samma sätt blir minutialäget för en förgrening förgreningspunkten för linjens mittskelett. Om de tre benen i åsen tunnas ner till en skelettbild som är en enda pixel bred är det skärningspunkten för de tre benen som är minutians läge.

När alla linjeslut har omvandlats till förgreningar, framställs alla minutiae i fingeravtrycksbilden som förgreningar. X- och Y-pixelkoordinaterna för skärningen av de tre benen i varje minutia kan direktformateras. Bestämning av minutiariktningen kan extraheras from varje skelettförgrening. De tre benen i varje skelettförgrening måste undersökas, och avslutningspunkten för varje ben bestämmas. Figur 6.1.2 illustrerar de tre metoder som används för att bestämma avslutningen på ett ben som grundar sig på en skanningsupplösning på 500 ppi.

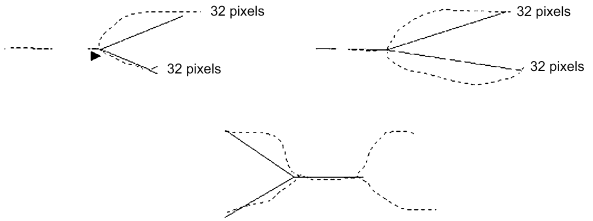
Avslutningen fastställs i enlighet med det som först inträffar. Pixelantalet grundar sig på en skanningsupplösning på 500 ppi. Olika skanningsupplösningar innebär olika pixelantal.

— Ett avstånd på .064 tum (den 32:a pixeln).

— Avslutningen på skelettbenet som inträffar mellan ett avstånd på .02 tum och .064 tum (den 10:e till den 32:a pixeln. Kortare ben används ej.

— En andra förgrening uppträder inom ett avstånd på .064 tum (före den 32:a pixeln).

Figur 6.1.2



Minutiavinkeln bestäms genom att man drar tre virtuella strålar som utgår från gaffelpunkten och fortsätter till avslutningen av varje ben. Den minsta av de tre vinklar som bildas av strålarna skärs av på mitten för att ange minutians riktning.

6.1.3 Koordinatsystem

Det koordinatsystem som används för att beskriva minutiae i ett fingeravtryck ska vara ett rätvinkligt koordinatsystem med två axlar. Läge för minutiae ska anges med deras x- och y-koordinater. Koordinatsystemet ska ha origo i det övre vänstra hörnet av den ursprungliga bilden, med x-axeln pekande åt höger och y-axeln pekande nedåt. Både x-koordinaten och y-koordinaten för en minutia ska anges i pixlar från origo. Det bör noteras att läget för origo och måttenheten inte stämmer med definitionen av typ 9-poster i ANSI/NIST-ITL 1-2000.

6.1.4 Minutiaeriktning

Vinklar ska uttryckas i vanlig matematisk form, med nollgrader åt höger och vinkelvärden som ökar moturs. Registrerade vinklar pekar i riktningen tillbaka längs åsen på en avslutning av åsen och mot dalens centrum på en förgrening. Enligt denna konvention avviker vinklarna 180 grader från vad som anges i definitionen poster av typ 9 i ANSI/NIST-ITL 1-2000.

6.2 *Fält i poster av typ 9, INCITS-378-format*

Samtliga fält i typ 9-poster ska registreras som ASCII-text. I denna posttyp med taggade fält tillåts inga binära fält.

6.2.1 Fält 9.001: Logisk postlängd (*Logical record length – LEN*)

I detta obligatoriska fält anges längden av den logiska posten som det sammanlagda antalet byte i varje fält i posten.

6.2.2 Fält 9.002: (Image Designation Character – IDC)

Detta obligatoriska fält om två positioner ska användas för att identifiera och ange läge för minutiaeuppgifterna. IDC i detta fält ska stämma överens med IDC i filinnehållsfältet i typ 1-posten.

6.2.3 Fält 9.003: (Impression Type – IMP)

Detta obligatoriska fält om en byte ska beskriva på vilket sätt informationen i fingeravtrycksbilden har erhållits. ASCII-värdet för rätt kod för avtryckstypen ur tabell 4 ska registreras i detta fält.

6.2.4 Fält 9.004: Minutiaeformat (*Minutiæ format – FMT*)

Detta fält ska innehålla "U" för att ange att minutiae är formaterade enligt M1-378. Även om informationen kan ha kodats enligt M1-378-standarden, måste samtliga fält i typ 9-posten förbli fält med ASCII-text.

6.2.5 Fält 9.126: CBEFF-information (*CBEFF-information*)

Detta fält ska innehålla tre uppgifter. Den första uppgiften ska ha värdet "27" (0x1B). Detta är en identifikation av ägaren av CBEFF-formatet som har tilldelats INCITS:s tekniska kommitté M1 av International Biometric Industry Association (IBIA). <US>-avgränsaren ska avgränsa denna uppgift från CBEFF-formattypen som har tilldelats värdet "513" (0x0201), vilket anger att denna post endast innehåller uppgifter om läge och vinkelriktning utan att

ange någon information ur Extended Data Block. <US>-avgränsaren ska avgränsa denna uppgift från CBEFF-produktidentifieraren (PID) som identifierar "ägaren" av kodningsutrustningen. Det är säljaren som fastställer detta värde. Det kan erhållas från IBIA:s webbplats (www.ibia.org) om det har publicerats på webben.

6.2.6 Fält 9.127: Identifikation av upptagningsutrustning (*Capture equipment identification*)

Detta fält ska innehålla två uppgifter skilda åt med <US>-avgränsaren. Den första uppgiften ska innehålla "APPF", om den utrustning som användes för att ursprungligen ta upp bilden var certifierad att överensstämma med bilaga F (Bildkvalitetsspecifikation för IAFIS, 29 januari 1999) till FBI:s specifikation för överföring av fingeravtryck i elektronisk form CJIS-RS-0010. Om utrustningen inte överensstämmer med denna specifikation, ska fältet innehålla teckensträngen "NONE". Den andra uppgiften ska innehålla upptagningsutrustningens identifikationsbegrepp (Capture Equipment ID), ett produktnummer för upptagningsutrustningen som tilldelats av säljaren. Värdet "0" anger att upptagningsutrustningens identifikationsbegrepp inte har rapporterats.

6.2.7 Fält 9.128: Horisontell linjelängd (*Horizontal Line Length – HLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet pixel i en enstaka horisontell linje i den överförda bilden. Storleken i horisontell led är begränsad till 65 534 pixel.

6.2.8 Fält 9.129: Vertikal linjelängd (*Vertical Line Length – VLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet horisontella linjer i den överförda bilden. Storleken i vertikal led är begränsad till 65 534 pixel.

6.2.9 Fält 9.130: Skalenheter (*Scale units – SLC*)

Detta obligatoriska ASCII-fält ska ange enhet för samplingsfrekvensen (pixeltätheten). "1" i detta fält anger pixel per tum, "2" anger pixel per centimeter. "0" i detta fält betyder att ingen enhet har angivits. I detta fall ger kvoten HPS/VPS pixelsidförhållandet (pixel aspect ratio).

6.2.10 Fält 9.131: Horisontell pixelskala (*Horizontal pixel scale – HPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i horisontell led, förutsatt att SLC innehåller "1" eller "2". I annat fall anger det den horisontella komponenten av pixelsidförhållandet (pixel aspect ratio).

6.2.11 Fält 9.132: Vertikal pixelskala (*Vertical pixel scale – VPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i vertikal led, förutsatt att SLC innehåller "1" eller "2". I annat fall anger det den vertikala komponenten av pixelsidförhållandet (pixel aspect ratio).

6.2.12 Fält 9.133: Fingervy (*Finger view*)

Detta obligatoriska fält innehåller vynumret för det finger postens uppgifter avser. Vynumren börjar på "0" och ökar till "15" med steglängden ett.

6.2.13 Fält 9.134: Fingerposition (*Finger Position – FGP*)

Detta fält ska innehålla koden för den fingerposition som lämnade informationen i denna typ 9-post. En kod mellan 1 och 10 från tabell 5, eller rätt handflatekod från tabell 10, ska användas för att ange finger- eller handflateposition.

6.2.14 Fält 9.135: Fingerkvalitet (*Finger quality*)

Detta fält ska ange den sammanlagda kvaliteten för uppgifterna om fingerminutiae med ett värde mellan 0 och 100. Detta tal sammanfattar fingerpostens kvalitet och avspeglar originalbildens kvalitet, kvaliteten vid extrahering av minutiae och andra operationer som kan påverka minutiaeposten.

6.2.15 Fält 1.136: Minutiaeantal (*Number of minutiae*)

I detta obligatoriska fält ska antalet minutiae som registrerats i denna logiska post anges.

6.2.16 Fält 9.137: Uppgifter om fingerminutiae (*Finger minutiæ data*)

Detta fält ska innehålla sex uppgifter åtskilda med <US>-avgränsaren. Det består av flera delfält där vart och ett innehåller detaljerna för enskilda minutiae. Det totala antalet minutiaedelfält måste stämma överens med antalet i fält 136. Den första uppgiften är minutiaeindexnummer, som ska initialiseras till "1" och ökas med "1" för varje tillkommande minutia i fingeravtrycket. Den andra och den tredje uppgiften är x-koordinaten och y-koordinaterna för minutiae i pixelenheter. Den fjärde uppgiften är minutiaevinkeln angiven i enheter om två grader. Detta värde ska vara icke-negativt mellan 0 och 179. Den femte uppgiften är minitiaetypen. Ett värde av "0" används för att representera minutiae av typen "ANNAN", ett värde av "1" för en åsavslutning och ett värde av "2" för en åsförgrening. Den sjätte uppgiften anger kvaliteten för varje minutiae. Värdet ska ligga mellan minst 1 och mest 100. Ett "0"-värde anger att kvalitetsvärde saknas. Varje delfält ska skiljas från nästa delfält med <RS>-avgränsaren.

6.2.17 Fält 9.138: Uppgifter om åsantal (*Ridge count information*)

Fältet består av en serie delfält där vart och ett innehåller tre uppgifter. Den första uppgiften i det första delfältet ska ange metoden för extrahering av antal åsar. "0" anger att metoden för att extrahera antalet åsar är okänd, liksom ordningen i posten. "1" anger att för varje centrumminutia har uppgifter om åsantal tagits fram till närmaste angränsande minutia i fyra kvadranter, och åsantal för varje centrumminutia har förtecknats tillsammans. "2" anger att för varje centrumminutia har uppgifter om åsantal tagits fram till närmaste grannminutia i fyra kvadranter, och åsantal för varje centrumminutia har förtecknats tillsammans. De återstående två uppgifterna i det första delfältet ska båda innehålla "0". Uppgifterna ska åtskiljas av <US>-avgränsaren. Följande delfält får centrumminutians indexnummer som första uppgift, indexnummer för angränsande minutiae som andra uppgift och antalet åsövergångar som tredje uppgift. Uppgifterna ska åtskiljas av <US>-avgränsaren.

6.2.18 Fält 9.139: Uppgifter om centrumpunkter (*Core information*)

Detta fält består av ett delfält för varje centrumpunkt i originalbilden. Varje delfält innehåller tre uppgifter. De första två uppgifterna innehåller x- och y-koordinatpositionerna i pixelenheter. Den tredje uppgiften innehåller centrumpunktens vinkel angiven i enheter om 2 grader. Detta värde ska vara icke-negativt mellan 0 och 179. Multipla centrumpunkter ska åtskiljas av <RS>-avgränsaren.

6.2.19 Fält 9.140: Deltauppgifter (*Delta information*)

Detta fält består av ett delfält för varje deltapunkt i originalbilden. Varje delfält innehåller tre uppgifter. De första två uppgifterna innehåller x- och y-koordinatpositionerna i pixelenheter. Den tredje uppgiften innehåller deltapunktens vinkel angiven i enheter av 2 grader. Detta värde ska vara icke-negativt mellan 0 och 179. Multipla centrumpunkter ska åtskiljas av <RS>-avgränsaren.

7. ***Post typ 13: Bilder av latenta avtryck med varierande upplösning***

Logisk post av typ 13 med taggade fält ska innehålla data från bilder av latenta avtryck. Dessa bilder är avsedda att överföras till organ som automatiskt extraherar eller använder mänsklig intervention och behandling för att extrahera den önskade detaljinformationen från bilderna.

Uppgifter om skanningsupplösning, bildstorlek och andra parametrar som krävs för att behandla bilden registreras som taggade fält inom posten.

Tabell 7: Post typ 13: Bilder av latenta avtryck med varierande upplösning

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	13 001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	13 002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	13 003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	13 004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
LCD	M	13 005	LATENT CAPTURE DATE	N	9	9	1	1	16

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
HLL	M	13 006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	13 007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	13 008	SCALE UNITS	N	2	2	1	1	9
HPS	M	13 009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	13 010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	13 011	COMPRESSION ALG-ORITHM	A	5	7	1	1	14
BPX	M	13 012	BITS PER PIXEL	N	2	3	1	1	10
FGP	M	13 013	FINGER POSITION	N	2	3	1	6	25
RSV		13 014 13 019	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
COM	O	13 020	COMMENT	A	2	128	0	1	135
RSV		13 021 13 199	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
UDF	O	13 200 13 998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	13 999	IMAGE DATA	B	2	—	1	1	—

Nyckel för teckentyp: N = numerisk, A = alfabetisk, AN = alfanumerisk, B = binär

7.1 *Fält i logisk post typ 4*

Följande stycken beskriver uppgifterna i vart och ett av fälten för logisk post typ 13.

Inom en logisk post typ 13 ska registreringar läggas in i numrerade fält. De första två fälten i posten måste vara i rätt ordning, och fältet med bilduppgifterna ska vara det sista fysiska fältet i posten. För varje fält i typ 13-posten förtecknas i tabell 7 koden "Beroende på tillgång på uppgifter" ("condition code") som obligatorisk "M" eller frivillig/valfri "O", fältnummer, fältbenämning, teckentyp, fältstorlek och förekomstgränser. Maximal storlek för fältet, uttryckt i antal byte och grundad på ett treställigt fältnummer, anges i sista kolumnen. När fler siffror används för fältnumret ökar också maximalt antal byte. De två registreringarna i fältstorlek per förekomst ("field size per occurrence") inkluderar alla teckenavgränsare i fältet. Maximalt antal byte ("Maximum byte count") inkluderar fältnummer, uppgifter och alla teckenavgränsare inklusive <GS>-avgränsaren.

7.1.1 Fält 13.001: Logisk postlängd (*Logical record length – LEN*)

I detta obligatoriska fält anges det totala antalet byte i hela logisk post typ 1. I fält 13.001 anges postens längd inklusive alla tecken i alla fält i posten samt uppgiftsavgränsare.

7.1.2 Fält 13.002: Bilddesigneringstecken (*Image Designation Character – IDC*)

Detta obligatoriska ASCII-fält ska användas för att identifiera bilduppgifterna om latent avtryck i posten. Detta IDC ska matcha IDC i fältet för filinnehåll (CNT) i typ 1-posten.

7.1.3 Fält 13.003: Avtryckstyp (*Impression Type – IMP*)

Detta obligatoriska fält om en eller två byte ska beskriva på vilket sätt bildinformationen om det latenta avtrycket har erhållits. Korrekt latentkod från tabell 4 (finger) eller tabell 9 (handflata) ska föras in i detta fält.

7.1.4 Fält 13.004: Källorgan (*Source agency/ORI – SRC*)

Detta obligatoriska ASCII-fält ska innehålla identifikation av den myndighet eller organisation som ursprungligen tog upp ansiktsbilden i posten. Normalt sett är det ursprungsorgansidentifieraren för det organ som tog upp bilden som ska stå i detta fält. Det består av två uppgifter i följande format: CC/*organ*.

Den första uppgiften består av Interpols landskod om två alfanumeriska tecken. Den andra uppgiften, *organ*, identifierar organet genom en sträng fri text om maximalt 32 alfanumeriska tecken.

7.1.5 Fält 13.005: Upptagningsdatum för latent avtryck (*Latent capture date – LCD*)

Detta obligatoriska ASCII-fält ska innehålla datum för upptagningen av den latenta bilden i posten. Datum skrivs som åtta siffror i formatet CCYYMMDD. CCYY-tecknen står för året för upptagningen av bilden. MM-tecknen är månadens tiotals- och enhetsvärden och DD-tecknen tiotals- och enhetsvärden för dagen i månaden. Till exempel står 20000229 för den 29 februari 2000. Fullständigt datum måste vara ett riktigt datum.

7.1.6 Fält 13.065: Horisontell linjelängd (*Horizontal Line Length – HLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet pixel i en enstaka horisontell linje i den överförda bilden.

7.1.7 Fält 13.007: Vertikal linjelängd (*Vertical Line Length – VLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet horisontella linjer i den överförda bilden.

7.1.8 Fält 13.008: Skalenheter (*Scale units – SLC*)

Detta obligatoriska ASCII-fält ska ange enhet för samplingsfrekvensen (pixeltätheten). "1" i detta fält anger pixel per tum, "2" anger pixel per centimeter. "0" i detta fält betyder att ingen enhet har angivits. I detta fall ger kvoten HPS/VPS pixelsidförhållandet (pixel aspect ratio).

7.1.9 Fält 13.009: Horisontell pixelskala (*Horizontal pixel scale – HPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i horisontell led, förutsatt att SLC innehåller "1" eller "2". I annat fall anger det den horisontella komponenten av pixelsidförhållandet (pixel aspect ratio).

7.1.10 Fält 13.010: Vertikal pixelskala (*Vertical pixel scale – VPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i vertikal led, förutsatt att SLC innehåller "1" eller "2". I annat fall anger det den vertikala komponenten av pixelsidförhållandet (pixel aspect ratio).

7.1.11 Fält 13.011: Komprimeringsalgoritm (*Compression algoritm – CGA*)

Detta obligatoriska ASCII-fält ska ange den algoritm som används för att komprimera gråskalebilder. Komprimeringskoderna anges i bilaga 7.

7.1.12 Fält 13.012: Bitar per pixel (*Bits per pixel – BPX*)

Detta obligatoriska ASCII-fält ska innehålla antalet bitar som används för en pixel. I detta fält står "8" för normala gråskalevärden från "0" till "255". Alla värden i detta fält som är större än "8" står för gråskalepixel med högre precision.

7.1.13 Fält 13.013: Fingerposition/handflateposition (*Finger/Palm Position – FGP*)

Detta obligatoriska taggade fält ska innehålla en eller flera av de möjliga finger-/handflatepositioner som kan matcha den latenta bilden. Det decimalkodsnummer som motsvarar den kända eller mest troliga fingerpositionen ska tas från tabell 5 eller den mest troliga handflatepositionen från tabell 10 och föras in som ett ASCII-delfält med ett eller två tecken. Ytterligare finger- och/eller handflatepositioner kan registreras genom att man lägger in alternerande positionskoder som delfält åtskilda av RS-avgränsaren. Koden "0" för "Okänt finger" ska användas för att registrera varje fingerposition från ett till tio. Koden "20" för "Okänd handflata" ska användas för att registrera varje handflateposition i förteckningen.

7.1.14 Fält 13.014-019: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

7.1.15 Fält 13.020: Kommentar (*Comment COM*)

Detta frivilliga fält kan användas för kommentarer eller annan information i ASCII-text med uppgifter om latent bild.

7.1.16 Fält 13.021-199: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

7.1.17 Fält 13.200-998: Användardefinierade fält (*User-defined fields – UDF*)

Dessa fält är användardefinierade fält och kommer att användas för framtida behov. Deras storlek och innehåll ska definieras av användaren i enlighet med det mottagande organet. Om de förekommer ska de innehålla information i ASCII-text.

7.1.18 Fält 13.999: Bilduppgifter (*Image data – DAT*)

Detta fält ska innehålla alla uppgifter från en upptagen latent bild. Det ska alltid få fältnummer 999 och måste vara det sista fysiska fältet i posten. Till exempel följs "13.999" av bilduppgifter i binärt format.

Varje pixel av okomprimerade gråskaleuppgifter ska normalt kvantifieras till åtta bitar (256 grå nivåer) i en enda byte. Om värdet i BPX-fältet 13.102 är större än eller mindre än "8" får man ett annat antal byte som krävs för att innehålla en pixel. Om komprimering används ska pixeluppgifterna komprimeras i enlighet med den komprimeringsteknik som anges i GCA-fältet.

7.2 *Avslutning post typ 13: Latenta bilder med varierande upplösning*

Omedelbart efter sista byte uppgifter från fält 13.199 ska för konsekvensens skull en <FS>-avgränsare användas för att avgränsa den från nästa logiska post. Denna avgränsare måste inkluderas i typ 13-postens längdfält.

8. ***Post typ 15: Bilder av handavtryck med varierande upplösning***

Det taggade fältet i logisk post typ 15 ska innehålla och användas för att utbyta uppgifter om handflateavtryck tillsammans med fasta och användardefinierade textinformationsfält avseende den digitaliserade bilden. Uppgifter om skanningsupplösning, bildstorlek och andra parametrar eller kommentarer som krävs för att behandla bilden registreras som taggade fält inom posten. Handflateavtrycksbilder som översänds till andra organ kommer att behandlas av de mottagande organen för att extrahera den önskade detaljinformation som krävs för matchning.

Bilduppgifterna fås direkt från en person med hjälp av en livescan-utrustning eller från en handflateavtrycksblankett eller annat medium som innehåller personens handflateavtryck.

Alla metoder som används för att få fram bilder av handflateavtrycket ska också medge upptagning av en uppsättning bilder för varje hand. Denna uppsättning ska inkludera handflatans yttre kant som en enda skannad bild och hela området för hela handen från handleden till fingertopparna som en eller två skannade bilder. Om två bilder används för att visa hela handflatan, ska den nedre bilden visa området från handleden till övre delen av området mellan fingrarna (tredje fingerleden) inklusive områdena kring handflatans tumvalk och lillfingervalk. Den övre bilden ska visa området från nedre delen av det interdigitala området till de översta fingertopparna. Detta ger tillräcklig överlappning mellan de två bilderna som båda visar handflateområdet mellan fingrarna. Genom att matcha åsstrukturen och detaljerna i detta gemensamma område kan en undersökare med tillförlitlighet konstatera att båda bilderna kom från samma handflata.

Eftersom en handavtryckstransaktion kan användas för olika ändamål, kan det innehålla ett eller flera unika bildområden registrerade från handflatan eller handen. En fullständig registrering av ett handflateavtryck från en individ inkluderar normalt handflatans yttre kant och fullständig/a bild/er av varje handflata. Eftersom en logisk bildpost med taggade fält kan innehålla endast ett binärt fält, kommer det att krävas en enda typ 15-post för varje handflatekant och en eller två typ 15-poster för varje fullständig handflata. Därför behövs det fyra till sex typ 15-poster för att visa personens handflateavtryck i en normal transaktion med handflateavtryck.

8.1 *Fält i logisk post typ 15*

Följande stycken beskriver uppgifterna i vart och ett av fälten för logisk post typ 15.

Inom en logisk post typ 15 ska registreringar läggas in i numrerade fält. De första två fälten i posten måste vara i rätt ordning, och fältet med bilduppgifterna ska vara det sista fysiska fältet i posten. För varje fält i typ 15-posten förtecknas i tabell 8 korskoden "Beroende av tillgång på uppgifter" ("condition code") som obligatorisk "M" eller frivillig/valfri "O", fältnummer, fältbenämning, teckentyp, fältstorlek och förekomstgränser. Maximal storlek för fältet, uttryckt i antal byte och grundad på ett treställigt fältnummer, anges i sista kolumnen. När fler siffror används för fältnumret ökar också maximalt antal byte. De två registreringarna i fältstorlek per förekomst ("field size per occurrence") inkluderar alla teckenavgränsare i fältet. Maximalt antal byte ("Maximum byte count") inkluderar fältnummer, uppgifter och alla teckenavgränsare inklusive GS-avgränsaren.

8.1.1 Fält 15.001: Logisk postlängd (*Logical record length – LEN*)

I detta obligatoriska ASCII-fält anges det totala antalet byte i hela den logiska posten av typ 15. I fält 15.001 ska anges postens längd inklusive alla tecken i alla fält i posten samt uppgiftsavgränsare.

8.1.2 Fält 15.002: Bildbenämningstecken (*Image Designation Character – IDC*)

Detta obligatoriska ASCII-fält ska användas för att identifiera uppgifterna om handflateavtrycksbilden i posten. Detta IDC ska matcha IDC i fältet för filinnehåll (CNT) i typ 1-posten.

8.1.3 Fält 15.003: Avtryckstyp (*Impression Type – IMP*)

Detta obligatoriska ASCII-fält om en byte ska ange på vilket sätt informationen i handavtrycksbilden har erhållits. Korrekt kod från tabell 9 ska föras in i detta fält.

8.1.4 Fält 15.004: Källorgan (*Source agency/ORI – SRC*)

Detta obligatoriska ASCII-fält ska innehålla identifikation av den myndighet eller organisation som ursprungligen tog upp ansiktsbilden i posten. Normalt sett är det ursprungsorgansidentifieraren för det organ som tog upp bilden som ska stå i detta fält. Det består av två uppgifter i följande format: CC/*organ*.

Den första uppgiften består av Interpols landskod om två alfanumeriska tecken. Den andra uppgiften, *organ*, identifierar organet genom en sträng fri text om maximalt 32 alfanumeriska tecken.

8.1.5 Fält 15.005: Upptagningsdatum för handflateavtrycket (*Palmprint capture date – PCD*)

Detta obligatoriska ASCII-fält ska ange datum för upptagningen av handflateavtrycket. Datum skrivs som åtta siffror i formatet CCYYMMDD. CCYY-tecknen står för året för upptagningen av bilden. MM-tecknen ska ange tiotals- och entalssiffran för månaden och DD-tecknen tiotals- och entalssiffran för dagen i månaden. Till exempel står 20000229 för den 29 februari 2000. Fullständigt datum måste vara ett verkligt datum.

8.1.6 Fält 15.006: Horisontell linjelängd (*Horizontal Line Length – HLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet pixlar i en enstaka horisontell linje i den överförda bilden.

8.1.7 Fält 15.007: Vertikal linjelängd (*Vertical Line Length – VLL*)

Detta obligatoriska ASCII-fält ska ange antalet horisontella linjer i den överförda bilden.

8.1.8 Fält 15.008: Skalenheter (*Scale units – SLC*)

Detta obligatoriska ASCII-fält ska ange enhet för samplingsfrekvensen (pixeltätheten). "1" i detta fält anger pixel per tum, "2" anger pixel per centimeter. "0" i detta fält betyder att ingen enhet har angivits. I detta fall ger kvoten HPS/VPS pixelsidförhållandet (pixel aspect ratio).

8.1.9 Fält 15.009: Horisontell pixelskala (*Horizontal pixel scale – HPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i horisontell led, förutsatt att SLC innehåller "1" eller "2". I annat fall anger det den horisontella komponenten av pixelsidförhållandet (pixel aspect ratio).

8.1.10 Fält 15.010: Vertikal pixelskala (*Vertical pixel scale – VPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i vertikal led, förutsatt att SLC innehåller "1" eller "2". I annat fall anger det den vertikala komponenten av pixelsidförhållandet (pixel aspect ratio).

Tabell 8: Post typ 15: Bilder av handflateavtryck med varierande upplösning

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min.	max.	
LEN	M	15 001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15 002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15 003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15 004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
PCD	M	15 005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15 006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15 007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15 008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15 009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15 010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15 011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15 012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15 013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15 014 15 019	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
COM	O	15 020	COMMENT	AN	2	128	0	1	128
RSV		15 021 15 199	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
UDF	O	15 200 15 998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	15 999	IMAGE DATA	B	2	—	1	1	—

Tabell 9: Handflateavtryckstyp

Description	Code
Live-scan palm	10
Nonlive-scan palm	11
Latent palm impression	12
Latent palm tracing	13
Latent palm photo	14
Latent palm lift	15

8.1.11 Fält 15.011: Komprimeringsalgoritm (*Compression algoritm – CGA*)

Detta obligatoriska ASCII-fält ska ange den algoritm som används för att komprimera gråskalebilder. "NONE" i detta fält anger att uppgifterna i denna post inte har komprimerats. För de uppgifter som ska komprimeras ska detta fält innehålla den metod som valts för komprimering av fingeravtrycksbilder av 10 fingrar. Giltiga komprimeringskoder definieras i bilaga 7.

8.1.12 Fält 15.012: Bitar per pixel (*Bits per pixel – BPX*)

Detta obligatoriska ASCII-fält ska innehålla antalet bitar som används för en pixel. I detta fält ska "8" stå för normala gråskalevärden från "0" till "255". Alla värden i detta fält som är större än eller mindre än "8" står för en gråskalepixel med högre respektive lägre precision.

Tabell 10: Handflatekoder, områden och storlekar

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Unknown Palm	20	28 387	139,7	203,2
Right Full Palm	21	28 387	139,7	203,2
Right Writer s Palm	22	5 645	44,5	127,0
Left Full Palm	23	28 387	139,7	203,2
Left Writer s Palm	24	5 645	44,5	127,0
Right Lower Palm	25	19 516	139,7	139,7
Right Upper Palm	26	19 516	139,7	139,7
Left Lower Palm	27	19 516	139,7	139,7
Left Upper Palm	28	19 516	139,7	139,7
Right Other	29	28 387	139,7	203,2
Left Other	30	28 387	139,7	203,2

8.1.13 Fält 15.013: Handavtrycksposition (Palmprint position – PLP)

Detta obligatoriska taggade fält ska innehålla den handavtrycksposition som matchar bilden av handflateavtrycket. Det decimalkodsnummer som motsvarar den kända eller mest troliga handavtrycksspositionen ska tas från tabell 10 och föras in som ett ASCII-delfält med ett eller två tecken. Tabell 10 listar också maximala bildområden och dimensioner för var och en av de möjliga positionerna för handavtrycken.

8.1.14 Fält 15.014-019: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

8.1.15 Fält 15.020: Kommentar (*Comment – COM*)

Detta frivilliga fält kan användas för kommentarer eller annan information i ASCII-text med uppgifter om handavtrycksbild.

8.1.16 Fält 15.021-199: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

8.1.17 Fält 15.200-998: Användardefinierade fält (*User-defined fields – UDF*)

Dessa fält är användardefinierade fält och kommer att användas för framtida behov. Deras storlek och innehåll ska definieras av användaren i enlighet med det mottagande organet. Om de förekommer ska de innehålla information i ASCII-text.

8.1.18 Fält 15.999: Biluppgifter (*Image data – DAT*)

Detta fält ska innehålla alla uppgifter om en upptagen handavtrycksbild. Det ska alltid tilldelas fältnummer 999 och måste vara det sista fysiska fältet i posten. Till exempel "15.999" följs av biluppgifter i binärt format. Varje pixel av okomprimerade gråskaleuppgifter ska normalt kvantifieras till åtta bitar (256 grå nivåer) i en enda byte. Om värdet i BPX-fältet 15.012 är större än eller mindre än "8" får man ett annat antal byte som krävs för att innehålla en pixel. Om komprimering används ska pixeluppgifterna komprimeras i enlighet med den komprimeringsteknik som anges i CGA-fältet.

8.2 *Avslutning post typ 15: Handavtrycksbilder med varierande upplösning*

Omedelbart efter sista byte av uppgifter från fält 15.999 ska för konsekvensens skull en <FS>-avgränsare användas för att avgränsa den från nästa logiska post. Denna avgränsare måste inkluderas i typ 15-postens längdfält.

8.3 *Ytterligare handavtrycksbilder av post typ 15 med varierande upplösning*

Ytterligare typ 15-poster kan inkluderas i filen. För varje ytterligare handavtrycksbild krävs en fullständig logisk post typ 15 tillsammans med <FS>-avgränsaren.

Tabell 11: Högsta för verifiering godtagna antal kandidater per sändning

Type of AFIS Search	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Maximum Number of Candidates	1	10	5	5	5	5	5

Sökningstyper:

TP/TP: tiofingersavtryck mot tiofingersavtryck

LP/TP: latent fingeravtryck mot tiofingersavtryck

LP/PP: latent handflateavtryck mot handflateavtryck

TP/UL: tiofingersavtryck mot olöst latent fingeravtryck

LT/UL: latent fingeravtryck mot olöst latent fingeravtryck

PP/ULP: handflateavtryck mot olöst latent handflateavtryck

LP/ULP: latent handflateavtryck mot olöst latent handflateavtryck

9. ***Bilagor till kapitel 2 (utbyte av finger- och handavtrycksuppgifter)***

9.1 *Bilaga 1 ASCII-koder för avgränsare*

ASCII	Position (1)	Description
LF	1/10	Separates error codes in field 2.074
FS	1/12	Separates logical records of a file
GS	1/13	Separates fields of a logical record
RS	1/14	Separates the subfields of a record field
US	1/15	Separates individual information items of the field or subfield

(1) Detta är positionen enligt definitionen i ASCII-standarden.

9.2 *Bilaga 2 Beräkning av alfanumeriskt kontrolltecken*

För TCN och TCR (Fält 1.09 och 1.10)

Det tal som motsvarar kontrolltecknet genereras enligt följande formel:

(YY * 10^8 + SSSSSSSS) Modulo 23

där YY and SSSSSSSS är de numeriska värdena av de sista två siffrorna för år respektive serienummer.

Kontrolltecknet genereras sedan ur tabellen nedan.

För CRO (Fält 2.010)

Det tal som motsvarar kontrolltecknet genereras enligt följande formel:

(YY * 10^6 + NNNNNN) Modulo 23

där YY and SSSSSSSS är de numeriska värdena av de sista två siffrorna för år respektive serienummer.

Kontrolltecknet genereras sedan ur tabellen nedan.

Kontrollteckentabell

1-A	9-J	17-T
2-B	10-K	18-U
3-C	11-L	19-V
4-D	12-M	20-W
5-E	13-N	21-X
6-F	14-P	22-Y
7-G	15-Q	0-Z
8-H	16-R	

9.3 *Bilaga 3 Teckenkoder*

7-bitars ANSI-kod för informationsutbyte

ASCII Character Set

+	0	1	2	3	4	5	6	7	8	9
30				!	"	#	$	%	&	'
40	(	)	*	+	,	—	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

9.4 *Bilaga 4 Sammanfattning av transaktioner*

Post typ 1 (obligatorisk)

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

Under villkorskolumnen:

O = frivilligt, M = obligatoriskt, C = beroende på om transaktionen är ett svar till ursprungsorganet

Post typ 2 (obligatorisk)

Identifier	Field Number	Field Name	CPS/ PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M
CNO	2.007	Case Number	—	M	C	—
SQN	2.008	Sequence Number	—	C	C	—
MID	2.009	Latent Identifier	—	C	C	—
CRN	2.010	Criminal Reference Number	M	—	C	—
MN1	2.012	Miscellaneous Identification Number	—	—	C	C
MN2	2.013	Miscellaneous Identification Number	—	—	C	C
MN3	2.014	Miscellaneous Identification Number	—	—	C	C
MN4	2.015	Miscellaneous Identification Number	—	—	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	—	—	M	—
ERM	2.074	Status/Error Message Field	—	—	—	M
ENC	2.320	Expected Number of Candidates	M	M	—	—

Under kolumnen "Condition":

O = frivilligt, M = obligatoriskt, C = beroende av tillgängliga uppgifter

* = om översändningen av uppgifterna är i enlighet med nationell lag (omfattas ej av beslut 2008/615/RIF)

9.5 *Bilaga 5 Post typ 1 definitioner*

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	1.001	Logical Record Length	N	1.001:230{GS}
VER	M	1.002	Version Number	N	1.002:0300{GS}
CNT	M	1.003	File Content	N	1.003:1{US}15{RS}2{US}00{RS}4{US}01{RS}4{US}02{RS}4{US}03{RS}4{US}04{RS}4{US}05{RS}4{US}06{RS}4{US}07{RS}4{US}08{RS}4{US}09{RS}4{US}10{RS}4{US}11{RS}4{US}12{RS}4{US}13{RS}4{US}14{GS}
TOT	M	1.004	Type of Transaction	A	1.004:CPS{GS}
DAT	M	1.005	Date	N	1.005:20050101{GS}
PRY	M	1.006	Priority	N	1.006:4{GS}
DAI	M	1.007	Destination Agency	1*	1.007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1.008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1.009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1.010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1.011:19.68{GS}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1.012:19.68{GS}
DOM	M	1.013	Domain Name	AN	1.013: INT-I{US}4.22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

Under kolumnen "Condition": O = frivillig, M = obligatorisk, C = beroende av tillgängliga uppgifter

Under teckentypkolumn: A = Alfa, N = Numerisk, B = Binär

1* tillåtna tecken för organets namn är ["0...9", "A...Z", "a...z", "_","'","." ," ", "-"]

9.6 *Bilaga 6 Post typ 2 definitioner*

Tabell A.6.1: CPS- och PMS-transaktion

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	M	2.010	Criminal Reference Number	AN	2.010:DE/E999999999{GS}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Tabell A.6.2: SRE-Transaktion

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	C	2.010	Criminal Reference Number	AN	2.010:NL/2222222222{GS}
MN1	C	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
RLS	M	2.064	Respondents List	AN	2.064:CPS{RS}I{RS}001/001{RS}999999{GS}

Tabell A.6.3: ERR-transaktion

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
MN1	M	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC - 1 FIELD 1 009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2 003 INVALID SYSTEM INFORMATION {GS}

Tabell A.6.4: MPS- och MMS-transaktion

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CNO	M	2.007	Case Number	AN	2.007:E999999999{GS}
SQN	C	2.008	Sequence Number	N	2.008:0001{GS}
MID	C	2.009	Latent Identifier	A	2.009:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123 {GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Under kolumnen "Condition": O = frivillig, M = obligatorisk, C = beroende av tillgängliga uppgifter

Under teckentypkolumn: A = Alfa, N = Numerisk, B = Binär

1* tillåtna tecken är ["0...9", "A...Z", "a...z", "_","."," ", "-"]

9.7 *Bilaga 7 Koder för gråskalekomprimering*

Komprimeringskoder

Compression	Value	Remarks
Wavelet Scalar Quantization Gray-scale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated December 19, 1997	WSQ	Algorithm to be used for the compression of grayscale images in Type-4, Type-7 and Type-13 to Type-15 records. Shall not be used for resolutions > 500dpi.
JPEG 2000 [ISO 15444/ITU T.800]	J2K	To be used for lossy and losslessly compression of grayscale images in Type-13 to Type-15 records. Strongly recommended for resolutions > 500 dpi

9.8 *Bilaga 8 E-postspecifikation*

För att förbättra det interna arbetsflödet måste ärenderubriken för en Prümtransaktion fyllas i med landskod (CC) för den medlemsstat som sänt meddelandet och även typ av transaktion (TOT-fältet 1.004).

Format: CC/*transaktionstyp*

Exempel: "DE/CPS"

Fältet för meddelandetext kan vara tomt.

KAPITEL 3: **Utbyte av uppgifter i fordonsregister**

1. ***Gemensam uppsättning uppgifter för automatiserad sökning i fordonsregister***

1.1 *Definitioner*

Definitionerna av obligatoriska och frivilliga uppgifter enligt artikel 16.4 är följande:

Obligatoriska uppgifter (M)

Uppgiften måste vidarebefordras när informationen är tillgänglig i en medlemsstats nationella register. Det finns därför en skyldighet att utbyta uppgifterna när de finns tillgängliga.

Frivilliga uppgifter (O)

Uppgiften får vidarebefordras när informationen är tillgänglig i en medlemsstats nationella register. Det finns därför ingen skyldighet att utbyta uppgifterna även om de finns tillgängliga.

Beteckningen (Y) används för varje uppgift i uppsättningen uppgifter som anses vara särskilt viktig med avseende på beslut 2008/615/RIF.

1.2 *Sökning på fordon/ägare/innehavare*

1.2.1 Sökkriterier

Det finns två olika sätt att söka efter uppgifterna, nämligen

— på fordonets identifieringsnummer (VIN), referensdatum och referenstid (frivilliga uppgifter),

— på numret på registreringsskylten, identifieringsnumret (VIN), referensdatum och referenstid (frivilliga uppgifter).

Med hjälp av dessa sökkriterier får man uppgifter om ett eller flera fordon. Om uppgifterna endast gäller ett fordon lämnas samtliga uppgifter i ett svar. Om fler än ett fordon har hittats kan den tillfrågade medlemsstaten själv besluta vilka uppgifter som ska lämnas ut: alla uppgifter eller endast de uppgifter som behövs för att begränsa sökningen (t.ex. av integritetsskäl eller prestandaskäl).

De uppgifter som behövs för att begränsa sökningen anges i punkt 1.2.2.1. I punkt 1.2.2.2 beskrivs den fullständiga uppsättningen uppgifter.

När man söker på identifieringsnummer, referensdatum och referenstid kan sökningen göras i en eller alla deltagande medlemsstater.

När man söker på registreringsnummer, referensdatum och referenstid måste sökningen göras i en viss medlemsstat.

Vanligen används nuvarande datum och tid för sökningen, men det är möjligt att göra en sökning med ett referensdatum och en referenstid i det förflutna. Om man gör en sökning med ett referensdatum och en referenstid i det förflutna, och historiska uppgifter inte finns tillgängliga i en viss medlemsstats register eftersom sådana uppgifter inte registreras över huvud taget, kan de aktuella uppgifterna komma upp som sökresultat med en angivelse om att det rör sig om aktuella uppgifter.

1.2.2 Uppsättning uppgifter

1.2.2.1 Uppgifter som behövs för att begränsa sökningen

Item	M/O [1]	Remarks	Prüm Y/N [2]
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1 [3]) e.g. Ford, Opel, Renault etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y

Item	M/O (1)	Remarks	Prüm Y/N (2)
EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y

(1) M = mandatory when available in national register, O = optional.
(2) All the attributes specifically allocated by the Member States are indicated with Y.
(3) Harmonised document abbreviation, see Council Directive 1999/37/EC of 29.4.1999.

1.2.2.2 Fullständig uppsättning uppgifter

Item	M/O (1)	Remarks	Prüm Y/N
Data relating to holders of the vehicle		(C.1 (2)) The data refer to the holder of the specific registration certificate.	
Registration holders' (company) name	M	(C.1.1.) separate fields will be used for surname, infixes, titles etc., and the name in printable format will be communicated	Y
First name	M	(C.1.2) separate fields for first name(s) and initials will be used, and the name in printable format will be communicated	Y
Address	M	(C.1.3) separate fields will be used for Street, House number and Annex, Zip code, Place of residence, Country of residence etc., and the Address in printable format will be communicated	Y
Gender	M	Male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date holdership	O	Start date of the holdership of the car. This date will often be the same as printed under (I) on the registration certificate of the vehicle.	N
End date holdership	O	End data of the holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: — is the vehicle owner — is not the vehicle owner — is not identified by the registration certificate as being the vehicle owner	N
Data relating to owners of the vehicle		(C.2)	
Owners' (company) name	M	(C.2.1)	Y
First name	M	(C.2.2)	Y

Item	M/O (1)	Remarks	Prüm Y/N
Address	M	(C.2.3)	Y
Gender	M	male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date ownership	O	Start date of the ownership of the car.	N
End date ownership	O	End data of the ownership of the car.	N
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1) e.g. Ford, Opel, Renault etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
Nature of the vehicle/EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y
Date of first registration	M	(B) date of first registration of the vehicle somewhere in the world	Y
Start date (actual) registration	M	(I) Date of the registration to which the specific certificate of the vehicle refers	Y
End date registration	M	End data of the registration to which the specific certificate of the vehicle refers. It is possible this date indicates the period of validity as printed on the document if not unlimited (document abbreviation = H).	Y
Status	M	scrapped, stolen, exported etc.	Y
Start date status	M		Y
End date status	O		N
kW	O	(P.2)	Y
Capacity	O	(P.1)	Y
Type of licence number	O	regular, transito etc.	Y
Vehicle document id 1	O	The first unique document ID as printed on the vehicle document	Y
Vehicle document id 2 (3)	O	A second document ID as printed on the vehicle document.	Y
Data relating to insurances			
Insurance company name	O		Y
Begin date insurance	O		Y
End date insurance	O		Y
Address	O		Y
Insurance number	O		Y

Item	M/O [1]	Remarks	Prüm Y/N
ID Number	O	An identifier that uniquely identifies the company.	N
Type of ID Number	O	The type of ID Number (e.g. number of the Chamber of Commerce)	N

[1] M = mandatory when available in national register, O = optional.
[2] Harmonised document abbreviation, see Council Directive 1999/37/EC of 29.4.1999.
[3] In Luxembourg two separate vehicle registration document ID's are used.

2. ***Datasäkerhet***

2.1 *Översikt*

Eucaris programapplikation används för säker kommunikation med övriga medlemsstater och kommunicerar med medlemsstaternas äldre back-end-system med hjälp av XML. Medlemsstaterna utbyter meddelanden genom att sända dem direkt till mottagaren. Varje medlemsstats datacentral är ansluten till EU:s Testa-nät.

De XML-meddelanden som sänds via nätet krypteras med krypteringstekniken SSL. De meddelanden som sänds till back-end-systemen är XML-meddelanden i klartext eftersom anslutningen mellan applikationen och back-end-systemen ska vara i en skyddad miljö.

Det tillhandahålls en klientapplikation som kan användas inom en medlemsstat för att söka i dess eget register eller i en annan medlemsstats register. Klienterna identifieras med hjälp av användar-ID/lösenord eller ett klientcertifikat. Anslutningen till en användare kan krypteras, men detta är varje enskild medlemsstats ansvar.

2.2 *Säkerhetsfunktioner i samband med meddelandeutbytet*

Säkerhetssystemet är baserat på en kombination av HTTPS och XML-signatur. Med detta alternativ används XML-signatur för att signera alla meddelanden som sänds till servern, och den som sänder meddelandet kan autentiseras genom att signaturen kontrolleras. Enkelsidig SSL (enbart ett servercertifikat) används för att skydda meddelandets konfidentialitet och integritet under överföringen och skyddar mot raderings-/replay- och insättningsattacker. Istället för skräddarsydd programvaruutveckling för att tillämpa dubbelsidig SSL, tillämpas XML-signatur. Användningen av XML-signatur ligger närmare färdplanen för webbtjänstgränssnitt än dubbelsidig SSL och är därför mer strategisk.

XML-signatur kan tillämpas på flera sätt men man har valt att använda tekniken som en del av *Web Services Security* (WSS). WSS anger hur XML-signatur ska användas. Eftersom WSS bygger på Soap-standarden är det logiskt att följa denna standard så långt det är möjligt.

2.3 *Säkerhetsfunktioner utan samband med meddelandeutbytet*

2.3.1 Autentisering av användare

Användare av Eucaris webbapplikation kan autentisera sig med hjälp av användarnamn och lösenord. Eftersom man använder Windows standardautentisering kan medlemsstaterna vid behov höja autentiseringsnivån för användarna genom att använda klientcertifikat.

2.3.2 Användarroller

Eucaris är anpassad till olika användarroller. Varje grupp av tjänster har en egen behörighetstilldelning. Användare som enbart har behörighet att använda "Eucarisavtalsfunktionen" får exempelvis inte använda "Prümfunktionen". Administratörstjänsterna är avskilda från de vanliga slutanvändarrollerna.

2.3.3 Loggning och spårning av meddelandeutbytet

Eucaris möjliggör loggning av alla typer av meddelanden. Genom en administratörsfunktion kan den nationella administratören bestämma vilka meddelanden som ska loggas: begäranden från slutanvändare, inkommande begäranden från andra medlemsstater, uppgifter som hämtats från de nationella registren osv.

Applikationen kan konfigureras så att den använder en intern databas eller en extern (Oracle) databas för denna loggning. Vilka meddelanden som måste loggas beror naturligtvis på loggningsmöjligheterna i andra delar av de äldre systemen och de anslutna klientapplikationerna.

Rubriken till varje meddelande innehåller information om den begärande medlemsstaten, den begärande organisationen inom den medlemsstaten och den berörda användaren. Skälet till begäran anges också.

Det är möjligt att spåra ett fullständigt meddelandeutbyte (t.ex. på begäran av den berörda medborgaren) med hjälp av den kombinerade loggningen i den begärande och tillfrågade medlemsstaten.

Loggningen konfigureras genom Eucaris webbklient (menu Administration, Logging configuration). Loggningsfunktionen utförs av grundsystemet. När loggningen är aktiverad lagras hela meddelandet (rubriken och meddelandetexten) i en loggningspost. Loggningsnivån kan ställas in enligt angiven tjänst eller enligt den meddelandetyp som passerar genom grundsystemet.

Loggningsnivåer

Följande loggningsnivåer är möjliga:

Privat – meddelandet loggas: Loggen är inte tillgänglig för sökning av loggningar, utan är endast tillgänglig på nationell nivå för revision och problemlösning.

Ingen – meddelandet loggas inte alls.

Typer av meddelanden

Informationsutbytet mellan medlemsstaterna består av flera meddelanden, som illustreras schematiskt i figuren nedan.

De möjliga meddelandetyperna (som i figuren visas för Eucaris grundsystem i medlemsstat X) är följande:

1. Begäran till grundsystemet_meddelande med begäran från klienten
2. Begäran till annan medlemsstat_meddelande med begäran från denna medlemsstats grundsystem
3. Begäran till denna medlemsstats grundsystem_meddelande med begäran från en annan medlemsstats grundsystem
4. Begäran till register i det äldre systemet_meddelande med begäran från grundsystemet
5. Begäran till grundsystemet_meddelande med begäran från register i det äldre systemet
6. Svar från grundsystemet_meddelande med begäran från klienten
7. Svar från annan medlemsstat_meddelande med begäran från denna medlemsstats grundsystem
8. Svar från denna medlemsstats grundsystem_meddelande med begäran från den andra medlemsstaten
9. Svar från register i det äldre systemet_meddelande med begäran från grundsystemet
10. Svar från grundsystemet_meddelande med begäran från register i det äldre systemet

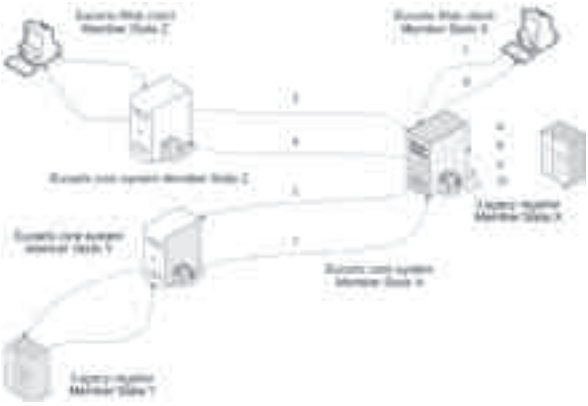
Följande typer av informationsutbyte visas i figuren:

— Begäran om information från medlemsstat X till medlemsstat Y – blå pilar. Denna begäran och svaret består av meddelandetyperna 1, 2, 7 respektive 6.

— Begäran om information från medlemsstat Z till medlemsstat X – röda pilar. Denna begäran och svaret består av meddelandetyperna 3, 4, 9 respektive 8.

— Begäran om information från registret i det äldre systemet till dess grundsystem (detta inkluderar även en begäran från en specialklient bakom registret i det äldre systemet) – gröna pilar. Denna typ av begäran består av meddelandetyperna 5 och 10.

Figur: Meddelandetyper för loggning



2.3.4 Säkerhetsmodul i maskinvara

Ingen säkerhetsmodul används i maskinvaran.

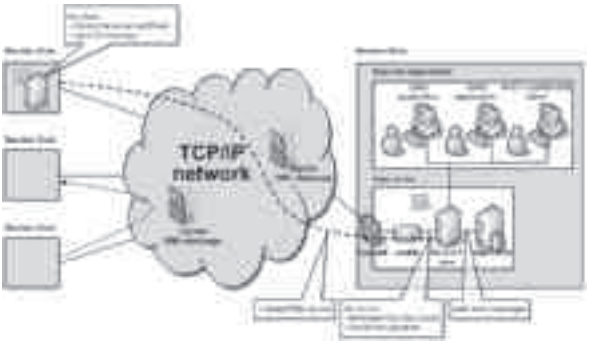
En säkerhetsmodul i maskinvaran (*HSM, Hardware Security Model*) ger ett gott skydd av den nyckel som används för att signera meddelanden och identifiera servrar. Detta bidrar till den allmänna säkerhetsnivån, men kostnaden är hög för inköp/underhåll av en HSM, och det finns inga krav på att använda en HSM som uppfyller nivå 2 eller 3 enligt FIPS-standarden 140-2. Eftersom man använder ett slutet nät som effektivt skyddar mot hot har man beslutat att inledningsvis inte använda någon HSM. Om en HSM blir nödvändig, t.ex. för att ackreditering, kan arkitekturen kompletteras med detta.

3. ***Tekniska villkor för informationsutbytet***

3.1 *Allmän beskrivning av Eucaris-applikationen*

3.1.1 Översikt

Eucaris-applikationen kopplar samman alla medlemsstater i ett meshnät där varje medlemsstat kommunicerar direkt med en annan medlemsstat. Ingen central komponent behövs för att etablera kommunikationen. Eucaris-applikationen hanterar säker kommunikation till de andra medlemsstaterna och kommunicerar med back-end-delen i äldre system hos medlemsstater som använder XML. Följande bild visualiserar denna arkitektur.



Medlemsstaterna utbyter meddelanden genom att sända dem direkt till mottagaren. En medlemsstats datacentral är kopplad till det nät som används för utbyte av meddelanden (Testa). För åtkomst av Testa-nätet ansluter sig medlemsstaterna till Testa via sin nationella nätport. En brandvägg ska användas för anslutning till nätet och en router ansluter Eucaris-applikationen till brandväggen. Beroende på vilket alternativ som väljs för att skydda meddelandena, används ett certifikat antingen av routern eller av Eucaris-applikationen.

En klientapplikation tillhandahålls som kan användas inom en medlemsstat för att söka i dess eget register eller andra medlemsstaters register. Klientapplikationen är ansluten till Eucaris. Klienterna identifieras med hjälp av användarID/lösenord eller ett klientcertifikat. Anslutningen till en användare i en extern organisation (t.ex. polisen) kan krypteras men detta är varje enskild medlemsstats ansvar.

3.1.2 Systemets tillämpningsområde

Eucaris-systemets tillämpningsområde är begränsat till processer som används i informationsutbytet mellan registreringsmyndigheterna i medlemsstaterna och en grundläggande presentation av denna information. Förfaranden och automatiserade processer i vilka informationen ska användas faller utanför systemets tillämpningsområde.

Medlemsstater kan välja att antingen använda Eucaris klientfunktion eller skapa sin egen skräddarsydda klientapplikation. I tabellen nedan anges vilka aspekter av Eucaris-systemet som obligatoriskt måste användas och/eller föreskrivs och vilka aspekter som är frivilliga och/eller som medlemsstaterna fritt kan fastställa.

EUCARIS aspects	M/O [1]	Remark
Network concept	M	The concept is an "any-to-any" communication.
Physical network	M	TESTA
Core application	M	The core application of EUCARIS has to be used to connect to the other Member States. The following functionality is offered by the core: — Encrypting and signing of the messages; — Checking of the identity of the sender; — Authorization of Member States and local users; — Routing of messages; — Queuing of asynchronous messages if the recipient service is temporally unavailable; — Multiple country inquiry functionality; — Logging of the exchange of messages; — Storage of incoming messages
Client application	O	In addition to the core application the EUCARIS II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the EUCARIS organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the EUCARIS organisation and this Council Decision. The specifications can only be changed by the EUCARIS organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the EUCARIS organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

[1] M = mandatory to use or to comply with O = optional to use or to comply with.

3.2 *Funktionella och icke funktionella krav*

3.2.1 Generisk funktionalitet

I detta avsnitt har de huvudsakliga generiska funktionerna beskrivits i allmänna termer

Nr	Beskrivning
1.	Systemet gör det möjligt för medlemsstaternas registreringsmyndigheter att utbyta begäranden och svar på ett interaktivt sätt.
2.	Systemet innehåller en klientapplikation som möjliggör för slutanvändare att översända sina begäranden och presentera svarsinformationen för manuell behandling.
3.	Systemet underlättar "rundsändning", vilket gör att en medlemsstat kan översända en begäran till alla de övriga medlemsstaterna. De inkommande svaren konsolideras genom grundapplikationen i ett svarsmeddelande till klientapplikationen (denna funktionalitet kallas "Multiple Country Inquiry").
4.	Systemet kan hantera olika slags meddelanden. Användarroll, behörighetstilldelning, routing, signering och loggning definieras alla per specifik tjänst.
5.	Systemet gör det möjligt för medlemsstaterna att utbyta meddelanden satsvis eller meddelanden som innehåller ett stort antal begäranden eller svar. Dessa meddelanden behandlas asynkront.
6.	Systemet lägger asynkrona meddelanden i väntekö om den mottagande medlemsstaten tillfälligt inte är tillgänglig och garanterar leveransen så snart som mottagaren är uppkopplad igen.
7.	Systemet lagrar inkommande asynkrona meddelanden tills de kan behandlas.
8.	Systemet ger endast åtkomst till andra medlemsstaters Eucaris-applikationer, inte till individuella organisationer inom dessa andra medlemsstater, vilket innebär att varje registreringsmyndighet agerar som den enda nätporten mellan dess nationella slutanvändare och motsvarande myndigheter i de andra medlemsstaterna.
9.	Det är möjligt att definiera användare från olika medlemsstater på en enda Eucaris-server och att ge dem behörighet i enlighet med gällande bestämmelser i den medlemsstaten.
10.	Meddelandena innehåller också information om den begärande medlemsstaten, organisationen och slutanvändaren.
11.	Systemet underlättar loggning av utbytet av meddelanden mellan de olika medlemsstaterna och mellan huvudapplikationen och de nationella registreringssystemen.
12.	Systemet tillåter att en särskild sekreterare, som är en organisation eller en medlemsstat som explicit har utsetts att sköta denna uppgift, samlar in loggad information om meddelanden som sänts eller mottagits av samtliga deltagande medlemsstater i syfte att sammanställa statistikrapporter.
13.	Varje medlemsstat anger själv vilken loggad information som ska göras tillgänglig för sekreteraren och vilken information som är "privat".
14.	Systemet tillåter varje medlemsstats nationella administratörer att ta fram utdrag ur användbar statistik.
15.	Systemet möjliggör tillägg av nya medlemsstater genom enkla administrativa åtgärder.

3.2.2 Användbarhet

Nr	Beskrivning
16.	Systemet tillhandahåller ett gränssnitt för automatiserad behandling av meddelanden med hjälp av back-end-delen i äldre system och möjliggör integration av användargränssnittet i dessa system (skräddarsytt användargränssnitt).
17.	Systemet är lätt att lära sig, självförklarande och innehåller hjälptext.
18.	Systemet är dokumenterat för att bistå medlemsstaterna i fråga om integrering, operativa aktiviteter och framtida underhåll (t.ex. referensmanual, funktionell/operativ dokumentation, användarmanual, ...).
19.	Användargränssnittet är flerspråkigt och erbjuder möjligheter för slutanvändaren att välja ett favoritspråk.
20.	Användargränssnittet tillhandahåller redskap med hjälp av vilka den lokala administratören kan översätta både skärmbildsobjekt och kodad information till det nationella språket.

3.2.3 Tillförlitlighet

Nr	Beskrivning
21.	Systemet är utformat som ett robust och pålitligt operativsystem som tolererar fel som operatören begår och som klarar strömavbrott eller andra olyckor. Det måste vara möjligt att starta om systemet med ingen eller minimal förlust av data.
22.	Systemet måste ge stabila och reproducerbara resultat.
23.	Systemet är utformat så att det fungerar pålitligt. Det är möjligt att implementera systemet i en konfiguration som garanterar 98 % tillgänglighet (genom redundans, användning av backup-servrar, osv.) i all bilateral kommunikation.
24.	Det är möjligt att använda delar av systemet även när några komponenter inte fungerar (om medlemsstat C ligger nere kan fortfarande medlemsstaterna A och B kommunicera). Antalet enskilda felställen i informationskedjan bör minimeras.
25.	Återhämtningstiden efter ett allvarligt haveri bör vara mindre än en dag. Det bör vara möjligt att minimera den tid systemet ligger nere genom användning av fjärrstöd, t.ex. en central servicedesk.

3.2.4 Prestanda

Nr	Beskrivning
26.	Systemet kan användas 24x7. Detta tidsfönster (24x7) krävs då också av medlemsstaternas äldre system.
27.	Systemet reagerar snabbt på en användarbegäran oavsett bakgrundsaktivitet. Detta krävs också av parternas äldre system för att säkerställa en godtagbar svarstid. En total svarstid om maximalt 10 sekunder för en enstaka begäran är godtagbar.
28.	Systemet har utformats som ett fleranvändarsystem och på ett sådant sätt att bakgrundsaktivitet kan fortsätta medan användaren utför förgrundsaktivitet.
29.	Systemet har utformats så att det är skalbart i syfte att klara en potentiell ökning av antalet meddelanden när ny funktionalitet läggs till eller nya organisationer eller medlemsstater ansluter sig.

3.2.5 Säkerhet

Nr	Beskrivning
30.	Systemet lämpar sig (t.ex. beträffande dess säkerhetsåtgärder) för utbyte av meddelanden som innehåller integritetskänslig information (t.ex. bilägare/innehavare) som klassificeras som EU RESTREINT.
31.	Systemet upprätthålls på ett sådant sätt att obehörig åtkomst av information förhindras.
32.	Systemet innehåller en tjänst för hantering av de nationella slutanvändarnas rättigheter och tillstånd.
33.	Medlemsstaterna kan kontrollera sändarens identitet (på medlemsstatsnivå) genom XML-signering.
34.	Medlemsstater måste uttryckligen ge andra medlemsstater behörighet för att de ska kunna begära särskild information.
35.	Systemet tillhandahåller på applikationsnivå en fullständig säkerhets- och krypteringspolicy som är kompatibel med den säkerhetsnivå som krävs i sådana situationer. Informationens exklusivitet och integritet garanteras genom användning av XML-signering och kryptering genom SSL-tunnling.
36.	Allt informationsutbyte kan spåras genom loggning.
37.	Skydd mot raderingsattacker tillhandahålls (en tredje part raderar ett meddelande) och replay- eller insättningsattacker (en tredje part spelar upp eller sätter in ett meddelande).
38.	Systemet använder sig av TTP-certifikat (*Trusted Third Party*).
39.	Systemet kan hantera olika certifikat per medlemsstat beroende på typen av meddelande eller tjänst.

Nr	Beskrivning
40.	Säkerhetsåtgärderna på applikationsnivå är tillräckliga för att tillåta användning av icke ackrediterade nät.
41.	Systemet är förberett för användning av ny säkerhetsteknik såsom en XML-brandvägg.

3.2.6 Anpassbarhet

Nr	Beskrivning
42.	Systemet kan utökas med nya meddelanden och ny funktionalitet. Anpassningskostnaderna är minimala beroende på den centraliserade utvecklingen av applikationskomponenter.
43.	Medlemsstaterna kan definiera nya meddelandetyper för bilateral användning. Det krävs inte av alla medlemsstater att de ska kunna klara av alla typer av meddelanden.

3.2.7 Stöd och underhåll

Nr	Beskrivning
44.	Systemet tillhandahåller övervakningsfaciliteter för en central servicedesk och/eller operatörer när det gäller nätet och servrar i de olika medlemsstaterna.
45.	Systemet tillhandahåller faciliteter för fjärrstöd genom en central servicedesk.
46.	Systemet tillhandahåller faciliteter för problemanalys.
47.	Systemet kan utsträckas till att omfatta nya medlemsstater.
48.	Applikationen kan enkelt installeras av personal med ett minimum av IT-kvalifikationer och erfarenhet. Installationsproceduren ska så långt som möjligt vara automatiserad.
49.	Systemet tillhandahåller en permanent test- och acceptansmiljö.
50.	De årliga kostnaderna för underhåll och stöd har minimerats genom anslutning till marknadsstandarder och genom att utforma applikationen så att så lite stöd som möjligt krävs från en central servicedesk.

3.2.8 Krav på utformningen

Nr	Beskrivning
51.	Systemet är utformat och dokumenterat för en operativ livslängd på många år.
52.	Systemet har utformats så att det är oberoende av nätleverantören.
53.	Systemet står i överensstämmelse med existerande HW/SW i medlemsstaterna genom att interagera med de registreringssystem som använder öppna standarder för webbtjänstteknik (XML, XSD, Soap, WSDL, HTTP(s), webbtjänster, WSS, X.509, osv.).

3.2.9 Tillämpliga standarder

Nr	Beskrivning
54.	Systemet uppfyller dataskyddskraven i förordning (EG) nr 45/2001 (artiklarna 21, 22 och 23) och direktiv 95/46/EG.
55.	Systemet uppfyller IDA-standarderna.
56.	Systemet är anpassat för UTF8.

KAPITEL 4: **Utvärdering**

1. ***Utvärderingsförfarande i enlighet med artikel 20 (förberedelse av beslut enligt artikel 25.2 i beslut 2008/615/RIF)***

1.1 *Frågeformulär*

Den berörda rådsarbetsgruppen ska utarbeta ett frågeformulär beträffande vart och ett av de automatiserade utbytena av information i kapitel 2 i beslut 2008/615/RIF.

Så snart som en medlemsstat anser sig uppfylla de nödvändiga förutsättningarna för att dela information i de relevanta informationskategorierna ska den besvara det relevanta frågeformuläret.

1.2 *Testkörning*

I syfte att utvärdera resultatet av frågeformuläret ska de medlemsstater som vill börja dela information genomföra en testkörning tillsammans med en eller flera andra medlemsstater som redan delar information enligt rådsbeslutet. Testkörningen ska äga rum före eller kort tid efter utvärderingsbesöket.

Villkoren och arrangemangen kring denna testkörning ska fastställas av den berörda rådsarbetsgruppen och grunda sig på en i förväg träffad separat överenskommelse med den berörda medlemsstaten. De medlemsstater som deltar i testkörningen beslutar själva om de praktiska detaljerna.

1.3 *Utvärderingsbesök*

I syfte att utvärdera resultatet av frågeformuläret ska ett utvärderingsbesök äga rum i den medlemsstat som vill börja dela information.

Villkoren och arrangemangen kring denna testkörning kommer att fastställas av den berörda rådsarbetsgruppen och grunda sig på en i förväg träffad separat överenskommelse mellan den berörda medlemsstaten och utvärderingsteamet. Den berörda medlemsstaten ska ge utvärderingsteamet möjlighet att kontrollera det automatiserade informationsutbytet i den eller de informationskategorier som ska utvärderas, bland annat genom att organisera ett program för besöket som beaktar de önskemål som utvärderingsteamet framfört.

Inom en månad ska utvärderingsteamet sammanställa en rapport om utvärderingsbesöket och överlämna den till berörda medlemsstater för kommentarer. I förekommande fall ska utvärderingsgruppen revidera denna rapport på grundval av medlemsstaternas kommentarer.

Utvärderingsteamet ska bestå av högst tre experter, utsedda av de medlemsstater som deltar i det automatiserade informationsutbytet i de informationskategorier som ska utvärderas, som har erfarenhet beträffande den berörda informationskategorin, som har genomgått lämplig nationell säkerhetskontroll för att få handha dessa frågor och som är villiga att delta i åtminstone ett utvärderingsbesök i en annan medlemsstat.

Medlemmarna i utvärderingsteamet ska respektera den inhämtade informationens konfidentiella natur i samband med att de utför sin uppgift.

1.4 *Rapport till rådet*

En övergripande utvärderingsrapport som sammanfattar resultatet av frågeformulären, utvärderingsbesöket och testkörningen kommer att läggas fram för rådet för beslut i enlighet med artikel 25.2 i beslut 2008/615/RIF.

2. ***Utvärderingsförfarande enligt artikel 21***

2.1 *Statistik och rapport*

Varje medlemsstat ska samla in statistik över resultatet av det automatiserade informationsutbytet. I syfte att säkerställa jämförbarhet kommer statistikmodellen att fastställas av den berörda rådsarbetsgruppen.

Dessa statistikuppgifter kommer årligen att läggas fram för rådet, som ska göra en övergripande sammanfattning av det gångna året, och för kommissionen.

Dessutom kommer medlemsstaterna regelbundet att anmodas att inte underlåta att en gång per år tillhandahålla sådana ytterligare uppgifter om det administrativa, tekniska och finansiella genomförandet av automatiserat utbyte av information som behövs för analys och förbättringar av processen. På grundval av denna information kommer en rapport att sammanställas för rådet.

2.2 *Revidering*

Inom rimlig tid kommer rådet att granska den utvärderingsmekanism som beskrivs här och vid behov revidera den.

3. Expertmöten

Inom den berörda rådsarbetsgruppen kommer experter regelbundet att träffas för att organisera och genomföra de ovannämnda utvärderingsförfarandena samt dela med sig av sina erfarenheter och diskutera möjliga förbättringar. I tillämpliga fall kommer resultatet av dessa expertdiskussioner att införlivas med den rapport som det hänvisas till i punkt 2.1 ovan.

Departementsserien 2009

Kronologisk förteckning

1. Förstärkt integritetsskydd vid signalspaning. Fö.
2. Skyddade beteckningar på jordbruksprodukter och livsmedel. Jo.
3. Fordonsbesiktning. N.
4. Översyn av vissa mediemyndigheter – en effektivare administration. Ku.
5. Författningsändringar med anledning av VIS-förordningen. Ju.
6. Ekonomiska villkor för ledamöter av Europaparlamentet. Ju.
7. Effektivare regler och bättre beslutsunderlag för arbetsmarknadspolitiken. A.
8. Genomförandet av delar av Prümrådsbeslutet. Ju.

Departementsserien 2009

Systematisk förteckning