Regeringskansliet
Faktapromemoria 2011/12:FPM119

Direktiv om dataskydd på det brottsbekämpande området

Justitiedepartementet

2012-02-29

Dokumentbeteckning

KOM (2012) 10 slutlig
Förslag till Europaparlamentets och rådets direktiv om skydd för enskilda personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter

Sammanfattning

Den 25 januari 2012 presenterade kommissionen sitt förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Paketet omfattar dels en förordning med en generell reglering som ska ersätta dataskyddsdirektivet (direktiv 95/46/EG), dels ett nytt direktiv med särregler för den brottsbekämpande sektorn som ska ersätta det gällande dataskyddsrambeslutet (rambeslut 2008/977/RIF). Till skillnad från dataskyddsrambeslutet ska direktivet inte omfatta endast utbyte av information över gränserna utan även nationell personuppgiftsbehandling inom den brottsbekämpande sektorn.

Syftet med direktivet är att garantera en enhetlig och hög nivå på uppgiftsskyddet och underlätta utbytet av personuppgifter mellan behöriga myndigheter. Därigenom säkerställs ett effektivt straffrättsligt samarbete och polissamarbete. Direktivet ansluter i stor utsträckning till den reglering som gäller enligt dataskyddsrambeslutet. Nya inslag är bl.a. kravet på att, så långt det är möjligt, vid behandlingen skilja mellan personuppgifter som avser olika kategorier av personer och likaså mellan uppgifter med olika grad av riktighet och tillförlitlighet. En annan nyhet är skyldigheten för den personuppgiftsansvarige att utan dröjsmål, om möjligt inom 24 timmar, underrätta tillsynsmyndigheten om ett dataintrång har ägt rum. I den delen föreslås kommissionen få befogenhet att anta delegerade akter och genomförandeakter. Direktivet innehåller vidare vissa nya regler om de

nationella tillsynsmyndigheternas ställning, villkor och uppgifter samt om obligatoriskt ömsesidigt bistånd och samarbete dem emellan. Direktivet innehåller slutligen också gemensamma bestämmelser för rättsmedel, ansvar och sanktioner.

Direktivet påverkar regleringen i de s.k. registerförfattningar som gäller inom direktivets tillämpningsområde, t.ex. polisdatalagen (2010:361).

Regeringen anser att Sverige bör välkomna en reform av EU:s dataskyddsregelverk i syfte att åstadkomma ett heltäckande och effektivt skydd för personuppgifter. Det är viktigt att den kommande regleringen inte kommer i konflikt med de svenska grundlagarna, framförallt att offentlighetsprincipen inte inskränks. Reformen får inte försvåra de brottsbekämpande myndigheternas möjligheter att bedriva en effektiv verksamhet med hjälp av modern teknik. Det måste finnas tillräckligt utrymme för nödvändig särreglering på nationell nivå bl.a. mot bakgrund av medlemsstaternas vitt skilda lagstiftning och organisation när det gäller brottsbekämpning. Frågan om rättsakternas form behöver analyseras. Regeringen anser att det är att föredra om även den generella dataskyddsregleringen ges formen av ett direktiv.

Regeringen anser att det finns anledning att närmare analysera om kommissionens förslag till dataskyddsdirektiv i alla delar är förenligt med subsidiaritetsprincipen och regeringen avser att noga följa upp frågan under förhandlingens gång.

Regeringen anser att förslagets förenlighet med proportionalitetsprincipen i vissa avseenden kan ifrågasättas.

1 Förslaget

1.1 Ärendets bakgrund

Nuvarande EU-reglering på dataskyddsområdet består av flera olika rättsakter. Inom det som tidigare var den första pelaren gäller direktiv 95/46/EG (dataskyddsdirektivet). Direktivet har i svensk rätt genomförts dels genom personuppgiftslagen (1998:204), dels genom ett stort antal s.k. registerförfattningar som innehåller särreglering om behandling av personuppgifter för olika myndigheter och sektorer (till exempel rättsväsendets myndigheter).

Inom den före detta tredje pelaren gäller rambeslut 2008/977/RIF (dataskyddsrambeslutet), som reglerar behandling av personuppgifter inom området för polisiärt och straffrättsligt samarbete. Rambeslutet gäller endast behandling av uppgifter som utbyts mellan medlemsstaterna, däremot inte rent nationell behandling av personuppgifter. Arbete med att genomföra de ännu inte genomförda delarna av dataskyddsrambeslutet pågår.

Genom Lissabonfördraget infördes en ny rättslig grund för dataskyddsreglering i artikel 16 i fördraget om Europeiska unionens funktionssätt. Rätten till skydd av personuppgifter har även fått status som en självständig grundläggande rättighet (artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna).

I Stockholmsprogrammet[1], som antogs av Europeiska rådet under det svenska ordförandeskapet 2009, uppmanade rådet kommissionen att utvärdera EU:s olika dataskyddsinstrument och vid behov ta ytterligare initiativ på lagstiftningsområdet. Kommissionen betonade i sin handlingsplan för att genomföra Stockholmsprogrammet att EU måste se till att den grundläggande rätten till skydd för personuppgifter tillämpas på ett konsekvent sätt och att skyddet för den enskildes personuppgifter måste stärkas inom alla EU:s politikområden.[2]

Kommissionen presenterade den 4 november 2010 ett meddelande med en strategi för att stärka EU:s regler om dataskydd.[3] Kommissionen uppmanade berörda parter att lämna synpunkter på meddelandet och genomförde också ett offentligt samråd. Den 24 februari 2011 antogs rådsslutsatser om meddelandet. Europaparlamentet antog en initiativrapport i juli 2011.[4] Både rådet och parlamentet uttryckte sitt stöd för kommissionens strategi.

Den 25 januari 2012 presenterade kommissionen sitt förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Paketet omfattar dels en förordning med en allmän reglering som ska ersätta det nuvarande dataskyddsdirektivet, dels ett nytt direktiv med särregler för den brottsbekämpande sektorn som ska ersätta dataskyddsrambeslutet. Denna faktapromemoria behandlar det senare förslaget. Förslaget till dataskyddsförordning behandlas i faktapromemoria (2011/12:FPM117).

1.2 Förslagets innehåll

Syftet med kommissionens förslag till dataskyddsdirektiv för det brottsbekämpande området är att garantera en enhetlig och hög nivå på uppgiftsskyddet, öka det ömsesidiga förtroendet mellan polis och rättsliga myndigheter och därmed underlätta det fria flödet av uppgifter och samarbetet mellan myndigheterna. Reglerna ska skydda fysiska personers rätt till skydd för personuppgifter, samtidigt som de ska trygga utbytet av personuppgifter och underlätta samarbetet i kampen mot brottsligheten i Europa.

Direktivet är uppbyggt enligt samma struktur som förslaget till allmän dataskyddsförordning och ansluter i stor utsträckning till den reglering som

[1] EUT C 115, 4.5.2010, s.1.

[2] KOM (2010) 171 slutlig.

[3] KOM (2010) 609 slutlig.

gäller enligt dataskyddsrambeslutet. Framställningen nedan koncentreras till förslagets huvuddrag samt på viktigare likheter och skillnader gentemot gällande dataskyddsreglering (och i vissa fall gentemot förslaget till allmän dataskyddsförordning).

1.2.1 Direktivets omfattning - definitioner

Direktivet innehåller regler för behandling av personuppgifter som görs i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa påföljd för brott. Direktivet föreslås, till skillnad mot dataskyddsrambeslutet, omfatta inte endast utbyte av information över gränserna utan all nationell personuppgiftsbehandling för brottsbekämpande ändamål inom dessa sektorer. Däremot undantas motsvarande behandling av personuppgifter som sker hos EU-institutioner och EU-myndigheter som omfattas av förordning (EC) 45/2001 och annan specifik EU-lagstiftning.

Definitionerna av de begrepp som används i direktivet överensstämmer till stor del med de definitioner som finns i dataskyddsrambeslutet. Begreppet ”blockering” har bytts ut mot ”begränsning av behandling” och liksom i förordningsförslaget finns ett flertal nya definitioner av bl.a. genetiska och biometriska uppgifter samt hälsouppgifter.

1.2.2 Principer för personuppgiftsbehandling

Direktivet innehåller ett antal allmänna principer för personuppgiftsbehandling. De ansluter nära till vad som gäller enligt dataskyddsrambeslutet och förslaget till allmän dataskyddsförordning. Principerna har i jämförelse med motsvarande principer i förordningsförslaget i viss mån anpassats till de krav som ställs på de brottsbekämpande myndigheternas informationsbehandling vad gäller proportionaliteten och transparensen gentemot den enskilde.

Ett nytt inslag är kravet på att, så långt det är möjligt, skilja mellan personuppgifter som avser olika kategorier av personer, såsom misstänkta, dömda, brottsoffer, vittnen och andra. Uppgifterna ska även så långt möjligt särskiljas utifrån graden av riktighet och tillförlitlighet samt om de bygger på fakta eller på bedömningar. Dessa förslag är hämtade från kommissionens ursprungliga förslag till dataskyddsrambeslut och liknande regler finns till exempel i Europolrådsbeslutet (2009/371/RIF).

Direktivet ställer krav på att uppgiftsbehandlingen ska vara lagenlig. Behandlingen ska vara nödvändig för att en behörig myndighet ska kunna fullgöra en lagstadgad uppgift som överensstämmer med direktivets syfte eller en annan laglig skyldighet eller för att skydda den registrerades eller någon annans vitala intressen eller för att avvärja ett omedelbart förestående allvarligt hot mot den allmänna säkerheten. Direktivet förbjuder behandling av känsliga personuppgifter, utom i särskilt angivna fall. Förbudet mot behandling av känsliga personuppgifter gäller inte om behandlingen är

tillåten enligt lagstiftning som innehåller tillräckliga säkerhetsåtgärder, är nödvändig för att skydda den enskildes eller någon annans vitala intressen eller avser uppgifter som den enskilde själv har offentliggjort. Regleringen i denna del är mer detaljerad än i dataskyddsrambeslutet och undantagen är färre än i förordningsförslaget.

Slutligen finns det särskilda bestämmelser med krav på lagenlighet och skydd för den enskilde mot negativa effekter av uppgiftsbehandling som bygger enbart på automatiserad behandling av personuppgifter i syfte att kartlägga vissa personliga aspekter relaterade till den enskilde (så kallad profilering).

1.2.3 Den enskildes rättigheter

Direktivet preciserar den enskildes rättigheter och den personuppgiftsansvariges skyldighet att lämna information om bland annat vilka uppgifter som behandlas, ändamålet med behandlingen, hur länge uppgifterna ska lagras, vem som är mottagare av uppgifterna samt vilka möjligheter den enskilde har att klaga på uppgiftsbehandlingen och att begära rättelse, radering eller ”begränsning av behandling” av uppgifter. Den enskilde har också, i likhet med vad som redan gäller, rätt att få felaktiga uppgifter rättade samt att få uppgifter kompletterade. Vidare införs en rätt att få en kopia av de uppgifter som behandlas.

Medlemsstaterna ges befogenhet att för vissa särskilt uppräknade ändamål inskränka de flesta av rättigheterna och skyldigheterna i direktivet genom nationell lagstiftning. En förutsättning för att få införa sådana inskränkningar är dock att de är nödvändiga och proportionella i förhållande till det eftersträvade ändamålet. När personuppgifterna hanteras inom ramen för en förundersökning eller rättegång kan medlemsstaterna bestämma att den enskildes rättigheter ska tillgodoses i enlighet med nationell processlagstiftning.

1.2.4 Den personuppgiftsansvariges ansvar

Direktivet föreskriver att medlemsstaterna ska vidta åtgärder för att säkerställa att behandling av uppgifter som görs av den personuppgiftsansvarige, och för dennes räkning, uppfyller direktivets krav. Till exempel ska den personuppgiftsansvarige vidta tekniska och organisatoriska åtgärder som säkerställer att direktivets krav efterlevs (principen om ett ”inbyggt uppgiftsskydd”). Den personuppgiftsansvarige ska även säkerställa att behandlingen, som standard, endast får avse de personuppgifter som är nödvändiga i förhållande till syftet med behandlingen (principen om ”dataskydd som standard”). Kravet innebär att de personuppgiftsansvariga måste minimera mängden personuppgifter som samlas in och lagras.

Bestämmelserna är nya och snarlika de som finns i förordningsförslaget. Detsamma gäller kraven på medlemsstaterna att säkerställa att uppgiftsbehandling som utförs av annan för den personuppgiftsansvariges räkning uppfyller direktivets krav samt att båda uppfyller minimikrav på dokumentation, registrering/loggning och samarbete med tillsynsmyndigheten.

Reglerna om informationssäkerhet, det vill säga den personuppgiftsansvariges ansvar för det tekniska och organisatoriska skyddet av informationen, har tagits över nästan ordagrant från dataskyddsrambeslutet. En nyhet är skyldigheten för den personuppgifts-ansvarige att utan dröjsmål, om möjligt inom 24 timmar, underrätta tillsyns-myndigheten om ett dataintrång har ägt rum. Kommissionen ges befogenhet att anta delegerade akter för att precisera kriterier och krav för när detta ska ske och hur det ska gå till. I vissa fall krävs även att de enskilda som berörs av intrånget underrättas. Underrättelsen kan dock skjutas upp, begränsas eller utgå helt enligt samma grunder som gäller för inskränkning av den enskildes rätt till information i allmänhet.

Slutligen föreskriver direktivet att medlemsstaterna ska vidta åtgärder för att den personuppgiftsansvarige ska utse ett dataskyddsombud, hur ombudet ska utses och vilken ställning och vilka uppgifter ombudet ska ha.

1.2.5 Överföring av personuppgifter till tredjeländer eller internationella organisationer

Direktivet anger förutsättningarna för överföring (och vidare överföring) av personuppgifter till tredjeländer eller till internationella organisationer utanför EU. Överföring får endast ske inom ramen för direktivets syfte och endast om mottagandelandet kan säkerställa en adekvat skyddsnivå för uppgifterna. Som huvudregel får överföring endast ske om kommissionen har beslutat att ett tredjeland uppfyller kraven, eller, i avsaknad av ett sådant beslut, om lämpliga skyddsåtgärder har vidtagits. Direktivet medger vissa undantag och anger förfaranden som ska tillämpas om kommissionen inte har fattat något sådant beslut. Direktivet fastställer också kriterier för kommissionens bedömning av en adekvat eller icke-adekvat skyddsnivå.

1.2.6 Tillsynsmyndigheter

Direktivet innehåller regler om de nationella tillsynsmyndigheternas ställning och uppgifter, villkoren för deras ledamöter samt tystnadsplikt och sanktioner.

En särskild arbetsuppgift för tillsynsmyndigheterna är att i vissa fall utöva rätten till tillgång för den registrerades räkning och att kontrollera att uppgiftsbehandlingen är tillåten.

Direktivets krav på förhandssamråd med tillsynsmyndigheten är strängare än motsvarande krav i den allmänna förordningen, vilket innebär att sådant

samråd måste genomföras oftare inom den brottsbekämpande sektorn än inom annan verksamhet.

Direktivet innehåller också bestämmelser om samarbete mellan medlemsstaternas tillsynsmyndigheter, bl.a. i form av obligatoriskt ömsesidigt bistånd. Europeiska dataskyddsstyrelsen, som föreslås inrättas genom den allmänna dataskyddsförordningen, ska enligt direktivet utöva sina uppgifter även i fråga om behandling av personuppgifter inom det brottsbekämpande området.

1.2.7 Rättsmedel, ansvar och sanktioner

Direktivet kräver att medlemsstaterna ger den enskilde rätt att klaga hos en nationell tillsynsmyndighet om den enskilde anser att behandlingen av dennes personuppgifter inte följt direktivets regler. Samma rätt tillkommer organisationer och sammanslutningar som har inrättats enligt nationell lagstiftning och som har till syfte att bevaka skyddet för den personliga integriteten. Det slås även fast att alla fysiska och juridiska personer ska ha rätt att överklaga tillsynsmyndighetens beslut om beslutet rör dem.

Den enskilde ska dessutom ges rättsmedel för att kunna förplikta tillsynsmyndigheten att agera utifrån ett klagomål som framförts dit. Den enskilde ska, i likhet med vad som redan gäller, ha rätt att väcka talan i domstol mot en personuppgiftsansvarig.

Direktivet inför gemensamma bestämmelser för domstolsförfaranden, bl.a. rättigheter för organ, organisationer eller sammanslutningar att företräda den enskilde inför domstol och rätt för tillsynsmyndigheter rätt att delta i rättsliga förfaranden. Medlemsstaterna är också skyldiga att säkerställa en snabb domstolsbehandling samt att det finns möjligheter att vidta interimistiska åtgärder för att avbryta pågående överträdelser och begränsa skadan av dessa.

För det fall en enskild drabbats av en skada på grund av en otillåten behandling av personuppgifter ska den enskilde ha rätt till skadestånd från den personuppgiftsansvarige. I övrigt ankommer det på medlemsstaterna att fastställa de sanktioner som ska komma ifråga vid överträdelser av direktivets bestämmelser. Sanktionerna måste dock vara effektiva, proportionerliga och avskräckande.

1.2.8 Ikraftträdande och förhållande till andra rättsakter och avtal

Direktivet riktar sig till medlemsstaterna och ersätter dataskyddsrambeslutet. Medlemsstaterna ska ha genomfört direktivet i sin nationella lagstiftning och tillämpa de nya reglerna senast två år efter direktivets ikraftträdande. Sådana bestämmelser om behandling av personuppgifter i syfte att förebygga, utreda, uppdaga eller lagföra brott eller verkställa påföljder för brott som finns i tidigare antagna rättsakter påverkas inte. Internationella överenskommelser

som medlemsstaterna träffat innan direktivet träder i kraft ska vid behov ändras inom fem år efter direktivets ikraftträdande.

1.3 Gällande svenska regler och förslagets effekt på dessa

Det föreslagna direktivet påverkar registerförfattningar inom direktivets tillämpningsområde, t.ex. polisdatalagen (2010:361). Den nya allmänna regleringen föreslås få formen av en förordning, vilket sannolikt skulle minska utrymmet för nationell reglering. Förordningen kommer att gälla för sådan verksamhet som inte är brottsbekämpande inom de myndigheter som berörs av direktivet, t.ex. polisens tillståndsverksamhet. I den nya polisdatalagen, som är resultatet av ca tio års lagstiftningsarbete, har det gjorts noggranna avvägningar mellan intresset av brottsbekämpning och skyddet av den personliga integriteten. Dataskyddsdirektivet kräver förändringar av den lagen och motsvarande lagar och förordningar för andra myndigheter i rättsväsendet (Tullverket, Kustbevakningen, åklagarväsendet, de allmänna domstolarna, Kriminalvården med flera).

1.4 Budgetära konsekvenser / Konsekvensanalys

Kommissionen har inte genomfört någon särskild konsekvensanalys över direktivförslaget utan hänvisar till den finansieringsöversikt som åtföljer förslaget till generell dataskyddsförordning. Det nya dataskyddsdirektivet kan bedömas innebära ekonomiska konsekvenser för myndigheterna i rättskedjan, bl.a. i form av ombyggnad av IT-system. Det är inte möjligt att i nuläget uppskatta de faktiska budgetära konsekvenserna. Regeringens utgångspunkt är dock att eventuella utökade kostnader ska rymmas inom stats- och EU-budgetens befintliga ramar.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen anser att Sverige bör välkomna en reform av EU:s dataskyddsregelverk i syfte att åstadkomma ett heltäckande och effektivt skydd för personuppgifter. Det finns dock vissa frågor av stort svenskt intresse som bör bevakas i samband med reformen.

Det är viktigt att den kommande regleringen inte kommer i konflikt med de svenska grundlagarna, framförallt att offentlighetsprincipen inte inskränks.

Det är också viktigt att den EU-rättsliga dataskyddsregleringen inte medför att de brottsbekämpande myndigheternas möjligheter att bedriva en effektiv verksamhet med hjälp av modern teknik försvåras. Det måste alltjämt finnas ett tillräckligt utrymme för att på nationell nivå ha den reglering som krävs bl.a. mot bakgrund av grundläggande principer i brottmålsförfarandet liksom

medlemsstaternas vitt skilda lagstiftning och organisation när det gäller brottsbekämpning. Vilket utrymme för sådan nationell lagstiftning som den föreslagna dataskyddsreformen medger behöver analyseras närmare. Möjligheterna till vidare behandling bör inte inskränkas jämfört med vad som anges i det helt nyligen genomförda dataskyddsrambeslutet.

Även frågan om hur den generella och den sektorsspecifika regleringen kan samspela, beroende på vilken form rättsakterna får, behöver analyseras. Regeringen ställer sig positiv till att regleringen för det brottsbekämpande området ges formen av ett direktiv och inte en förordning och anser att det är att föredra om även den generella dataskyddsregleringen ges formen av ett direktiv.

Vissa delar av förslaget, såsom vissa av reglerna om rätt till rättsmedel, behöver analyseras noga för att det ska vara möjligt att se om de är förenliga med svensk lagstiftning. En annan aspekt är att direktivet bör möjliggöra att behandlade uppgifter kan användas för exempelvis forskningsändamål.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaterna har ännu inte uttryckt några officiella ståndpunkter.

2.3 Institutionernas ståndpunkter

Institutionerna har ännu inte uttryckt några officiella ståndpunkter.

2.4 Remissinstansernas ståndpunkter

Förslaget till direktiv har nyligen remitterats och remisstiden går ut den 30 mars 2012. Inga synpunkter har ännu inkommit.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Den rättsliga grunden för förslaget är artikel 16.2 i fördraget om Europeiska unionens funktionssätt. Beslut fattas genom det ordinarie beslutsförfarandet, vilket betyder att det krävs kvalificerad majoritet i rådet samt enighet med Europaparlamentet för att anta det föreslagna direktivet.

3.2 Subsidiaritets- och proportionalitetsprincipen

Beträffande subsidiaritetsprincipen anför kommissionen att den grundläggande rätten till skydd av personuppgifter, som fastslås i artikel 8 i stadgan om de grundläggande rättigheterna, kräver att samma nivå av uppgiftsskydd ska gälla i hela unionen, både för uppgifter som utbyts mellan

medlemsstaterna och uppgifter som behandlas nationellt. Kommissionen pekar också på att det finns ett växande behov av att utbyta personuppgifter mellan medlemsstaternas brottsbekämpande myndigheter och att enhetliga dataskyddsregler kommer att bidra till att främja samarbetet. Kommissionen menar att det finns praktiska problem med att genomdriva dataskyddsregleringar och att det behövs samarbete organiserat på EU-nivå mellan medlemsstaterna och deras myndigheter för att säkerställa en enhetlig tillämpning och en hög skyddsnivå inom unionen. Vidare anses medlemsstaterna inte ensamma kunna minska problemen, särskilt inte de problem som uppstår på grund av splittring mellan medlemsstaternas nationella lagstiftningar. Därför menar kommissionen att det finns ett behov av att etablera ett harmoniserat och sammanhängande regelverk på EU-nivå, vilket med tanke på problemens gränsöverskridande karaktär anses mer effektivt än åtgärder på medlemsstatsnivå.

Kommissionen anför vidare att proportionalitetsprincipen har varit vägledande under förberedelsen av förslaget.

Regeringen anser att det finns anledning att närmare analysera om kommissionens förslag till dataskyddsdirektiv i alla delar är förenligt med subsidiaritetsprincipen och regeringen avser att noga följa upp frågan under förhandlingens gång.

Regeringen anser att förslagets förenlighet med proportionalitetsprincipen i vissa avseenden kan ifrågasättas. Några av förslagets bestämmelser kan till innehåll och form möjligen anses gå utöver vad som är nödvändigt för att nå målen i fördragen, några kan eventuellt även anses falla utanför unionens kompetens. Det gäller t.ex. vissa av bestämmelserna om personuppgiftsombud, tillsynsmyndigheter och rättsmedel. Även dessa frågor behöver analyseras närmare och följas upp under förhandlingens gång.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Förslagen beslutas i enlighet med det ordinarie lagstiftningsförfarandet.

Förhandlingarna om förslaget till generell dataskyddsförordning inleddes i slutet av februari 2012 men det är ännu oklart om förhandlingarna om förslaget till dataskyddsdirektiv för den brottsbekämpande sektorn kommer att förhandlas parallellt eller först när förhandlingarna om förslaget till dataskyddsförordning har kommit en bit på väg.