



EUROPEISKA KOMMISSIONEN

Bryssel den 25.1.2012
SEK(2012) 73 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

som medföljer dokumentet

Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)

och

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

{COM(2012) 11 final}
{SEC(2012) 72 final}

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

som medföljer dokumentet

Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)

och

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

1. INLEDNING

Sedan EU:s nuvarande rättsliga ram om uppgiftsskydd antogs 1995 har den snabba utvecklingen inom teknik och i affärsvärlden medfört nya utmaningar för skyddet av personuppgifter. Omfattningen av datadelning och datainsamling har ökat dramatiskt. Tekniken gör det möjligt för både företag och myndigheter att i sitt arbete använda sig av personuppgifter i en omfattning utan tidigare motstycke. Enskilda personer gör alltmer personlig information tillgänglig, för allmänheten och globalt, utan att vara fullt medveten om de därmed förbundna riskerna.

Att bygga upp förtroendet för nätmiljön är avgörande för den ekonomiska utvecklingen. Bristande förtroende gör att konsumenterna tvekar att köpa produkter på nätet och använda nya tjänster, däribland offentliga e-förvaltningstjänster. Om man inte tar itu med denna brist på förtroende kommer den att fortsätta att bromsa utvecklingen av innovativ användning av ny teknik, att fungera som ett hinder för ekonomisk tillväxt och att hindra den offentliga sektorn från att skörda de potentiella frukterna av en digitalisering av sina tjänster.

Dessutom har Lissabonfördraget skapat, genom artikel 16 i EUF-fördraget, en ny rättslig grund för en moderniserad och övergripande strategi för uppgiftsskydd och den fria rörligheten för personuppgifter, som också omfattar polissamarbete och straffrättsliga samarbete.

2. PROBLEMFORMULERING

I konsekvensbedömningen presenteras och analyseras tre viktiga problemområden:

2.1. Problem 1: Hinder för företag och myndigheter till följd av fragmentering, rättsosäkerhet och inkonsekvent verkställighet

Trots direktivets mål att säkerställa en likvärdig nivå för uppgiftsskyddet inom EU finns det fortfarande avsevärda skillnader mellan bestämmelserna i de olika medlemsstaterna. Därför kan registeransvariga behöva hantera 27 olika nationella lagar och krav inom EU. Resultatet är ett fragmenterat rättsligt klimat, och detta har skapat rättsosäkerhet och olika skydd för enskilda personer. Detta har gett upphov till onödiga kostnader och **administrativa bördor** (som uppgår till **cirka 3 miljarder euro per** år i grundscenariot) för företag och utgör ett hinder för företag, inklusive små och medelstora företag, som är verksamma på den inre marknaden och som skulle vilja utvidga sin verksamhet över gränserna.

Resurserna och befogenheterna hos de nationella myndigheter som ansvarar för uppgiftsskydd varierar dessutom avsevärt mellan medlemsstaterna. I vissa fall innebär detta att de är oförmögna att utföra sina tillsynsuppgifter på ett tillfredsställande sätt. Samarbete mellan dessa myndigheter på europeisk nivå – via den befintliga rådgivande gruppen (artikel 29-gruppen) – leder inte alltid till enhetlig tillsyn och behöver därför också förbättras.

2.2. Problem 2: Svårigheter för enskilda personer att behålla kontrollen över sina personuppgifter

Med tanke på avsaknaden av harmonisering i nationell lagstiftning om uppgiftsskydd och de olika befogenheterna för nationella dataskyddsmyndigheter, är det svårare för enskilda personer att utöva sina rättigheter i vissa medlemsstater än i andra, särskilt i nätsammanhang.

Till detta kommer att enskilda personer har förlorat kontrollen över sina egna uppgifter – dels enbart på grund av mängden uppgifter som delas varje dag och dels på grund av det faktum att de ofta inte är fullt medvetna om att uppgifterna samlas in. Många européer anser att utlämnandet av personuppgifter alltmer utgör en del av det moderna livet¹, men 72 % av internetanvändarna i Europa är fortfarande oroliga över att de ombeds lämna ut alltför mycket personuppgifter online, och de vet ofta inte hur de kan utöva sina rättigheter på nätet.

2.3. Problem 3: Brister och inkonsekvenser i skyddet av personuppgifter inom ramen för polissamarbete och straffrättsliga samarbete

Direktivets tillämpningsområde, som baseras på en rättslig grund för den inre marknaden, uteslöt särskilt polissamarbete och straffrättsligt samarbete. Det rambeslut som antogs 2008 för att reglera databehandling inom ramen för polissamarbete och straffrättsligt samarbete återspeglar särdragen i EU:s ”pelarstruktur” (före Lissabon) och kännetecknas av **en begränsad räckvidd och diverse andra brister**, något som ofta leder till rättsosäkerhet för enskilda personer och brottsbekämpande myndigheter, liksom till praktiska svårigheter med genomförandet. Dessutom erbjuder rambeslutet en rad olika möjligheter till undantag från allmänna principer för uppgiftsskydd på nationell nivå, och detta innebär att dessa principer inte harmoniseras. Detta riskerar inte bara att undergräva själva syftet med sådana principer – och därmed att negativt påverka enskilda personers grundläggande rättighet till skydd av personuppgifter på detta område – utan hindrar också ett smidigt utbyte av personuppgifter mellan relevanta nationella myndigheter.

¹ Se Special Eurobarometer 359 – *Attitudes on Data Protection and Electronic Identity in the European Union*, juni 2011, s. 23.

3. SUBSIDIARITETS- OCH PROPORTIONALITETSANALYS

Mot bakgrund av de ovan skisserade problemen visar subsidiaritetsanalysen att det är nödvändigt att vidta åtgärder på EU-nivå av följande skäl:

- Rätten till skydd av personuppgifter fastslås i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Artikel 16 i EUF-fördraget utgör den rättsliga grunden för antagandet av EU-bestämmelser om uppgiftsskydd.
- Personuppgifter kan överföras över nationsgränserna – både inom EU och till tredjeländer – i snabbt ökande omfattning. Dessutom finns det praktiska problem med genomförandet av uppgiftsskyddslagstiftningen och ett behov av samarbete mellan medlemsstaterna och deras myndigheter, vilket måste organiseras på EU-nivå för att säkerställa den nödvändiga enhetligheten och en hög skyddsnivå inom unionen.
- Medlemsstaterna kan inte på egen hand minska problemen i nuvarande situation. Detta gäller särskilt de problem som uppstår på grund av fragmenteringen i fråga om de nationella bestämmelser som införts för att genomföra EU:s rambestämmelser för uppgiftsskydd.
- Det skulle visserligen vara möjligt för medlemsstaterna att anta strategier som garanterar att denna rättighet inte kränks, men i avsaknad av gemensamma EU-bestämmelser skulle detta inte uppnås på ett enhetligt sätt och det skulle skapa restriktioner för gränsöverskridande flöden av personuppgifter.

De **planerade åtgärderna är proportionerliga** eftersom de ligger inom unionens behörighetsområde i enlighet med fördragen och är nödvändiga för att säkerställa en enhetlig tillämpning av EU:s lagstiftning och ett faktiskt och jämbördigt skydd av enskilda personers grundläggande rättigheter. Åtgärder på EU-nivå är nödvändiga för att även fortsättningsvis säkerställa trovärdighet och en hög nivå på uppgiftsskyddet i en globaliserad värld, samtidigt som det fria flödet av uppgifter upprätthålls. En väl fungerande inre marknad kräver att bestämmelserna säkerställer lika villkor för de ekonomiska aktörerna.

4. MAL

De tre främsta **politiska målen** är

- att **stärka uppgiftsskyddet med avseende på den inre marknaden** genom att minska fragmenteringen, förstärka enhetligheten och **förenkla** lagstiftningen, och därigenom eliminera onödiga kostnader och **minska de administrativa bördorna**,
- att **öka effektiviteten i den grundläggande rättigheten till uppgiftsskydd och ge enskilda personer kontroll över sina uppgifter**,
- att **stärka samstämmigheten i EU:s ram för uppgiftsskydd**, även inom området polissamarbete och rättsligt samarbete inom straffrättsliga frågor, med fullt beaktande av Lissabonfördragets ikraftträdande.

5. ALTERNATIV

5.1. Alternativ 1: Mjuka åtgärder

Detta alternativ skulle huvudsakligen bestå av **tolkningsmeddelanden från kommissionen, tekniska stödinstrument och finansiering** – samt åtgärder som **främjar standardisering och självreglering** – för att stärka registeransvarigas praktiska genomförande av befintliga bestämmelser och för att öka enskilda personers medvetenhet. Kommissionen skulle föreslå **endast mycket begränsade lagändringar** för att klargöra befintliga begrepp i direktivet och för att inrikta sig på särskilda frågor som inte kan hanteras effektivt på något annat sätt. Detta alternativ skulle vara relevant endast för problem 1 och 2.

De begränsade lagändringarna skulle innebära att man uttryckligen inför principerna om öppenhet och uppgiftsminimering samt en rättslig grund för ”bindande företagsbestämmelser” för internationella överföringar.

5.2. Alternativ 2: En moderniserad rättslig ram

Kommissionen skulle lägga fram **lagstiftningsförslag för att ytterligare harmonisera de materiella reglerna**, klargöra särskilda bestämmelser och undanröja inkonsekvenser som orsakats av olika förhållningssätt i medlemsstaterna. Dessa förslag skulle åtgärda problem 1 och 2 eftersom de dels skulle **underlätta dataflöden inom EU och från EU till tredjeländer**, dels **klargöra och stärka enskilda personers rättigheter** (t.ex. rätten till tillgång, ”rätten att bli bortglömd”, tydligare bestämmelser om samtycke och om anmälan av uppgiftsbrott) **och förstärka ansvaret – och ”ansvarsskyldigheten” – hos registeransvariga och registerförare** (t.ex. genom att införa, där det är lämpligt, en skyldighet att utse uppgiftsskyddsombud eller att utföra konsekvensbedömningar för uppgiftsskydd). Detta alternativ skulle framförallt skapa **en enda kontaktpunkt** för registeransvariga (dvs. en enda lag och en enda tillsynsmyndighet med ansvar för uppgiftsskydd). Allmänna anmälningskrav skulle förenklas (dvs. ”grundläggande registrering”). Det skulle också **stärka dataskyddsmyndigheternas oberoende och harmonisera deras befogenheter**. Samarbetet och det ömsesidiga biståndet mellan dataskyddsmyndigheter skulle stärkas, bland annat med hjälp av en ny **”mekanism för enhetlighet”** som omfattar både (den nyligen inrättade) ”Europeiska dataskyddsstyrelsen” och kommissionen.

När det gäller uppgiftsskydd inom området polissamarbete och straffrättsligt samarbete (problem 3) skulle kommissionen lägga fram förslag om att ersätta rambeslutet med ett **nytt instrument med utvidgat tillämpningsområde**. Vidare skulle kommissionen ta itu med **de största bristerna och felen**, för att både stärka enskilda personers rättigheter och underlätta samarbetet mellan brottsbekämpande myndigheter, samtidigt som hänsyn tas till särdragen hos brottsbekämpningssektorn.

5.3. Alternativ 3: Detaljerad lagstiftning på EU-nivå

Detta alternativ skulle omfatta de flesta inslagen i alternativ 2 samt **mycket mer detaljerad EU-lagstiftning**, däribland sektorsspecifik lagstiftning (t.ex. inom hälso- och sjukvårdsområdet), och en **centraliserad tillsynsstruktur på EU-nivå** (dvs. inrättandet av en EU-myndighet för dataskydd). Det skulle också innebära undanröjande av allmänna anmälningskrav (utom för förhandskontroll av behandling som medför risker), inrättande av ett EU-omfattande certifieringssystem för processer och produkter som uppfyller

uppgiftsskyddsbestämmelserna samt fastställande av harmoniserade EU-omfattande straffrättsliga påföljder för brott mot bestämmelserna om uppgiftsskydd. Samtycke skulle definieras som "huvudsaklig grund" för databehandling.

Beträffande polissamarbete och straffrättsligt samarbete skulle alternativet, utöver de materiella åtgärder som ingår i alternativ 2, omfatta fastställande av detaljerade bestämmelser för enskilda personers rätt till tillgång (alltid direkt). Det skulle också innebära **ändringar av relevanta bestämmelser i alla befintliga instrument som tidigare omfattades av den tredje pelaren**, så att de anpassas fullt ut till de nya och utvidgade harmoniserade bestämmelserna.

6. KONSEKVENSBEDÖMNING

6.1. Alternativ 1: Mjuka åtgärder

Kommissionens tolkningsmeddelanden om bestämmelser i direktivet skulle inte vara bindande och skulle därför ha **endast begränsad inverkan när det gäller att minska rättsosäkerheten och kostnaderna**. Mer självreglering på EU-nivå skulle kunna bidra till att ge större rättslig klarhet för registeransvariga inom vissa sektorer, men **det skulle inte vara tillräckligt** för att säkerställa en effektiv och enhetlig tillämpning av bestämmelserna i avsaknad av en underliggande tydlig och harmoniserad rättslig ram på EU-nivå.

Medvetandehöjande kampanjer skulle hjälpa de enskilda att få bättre kunskap om sina rättigheter avseende uppgiftsskydd och att bättre förstå hur man praktiskt kan utöva dessa rättigheter. Detta är emellertid **inte tillräckligt** för att enskilda personer ska kunna ta reda på vilka rättigheter de har om dessa rättigheter inte är klart definierade i lagen. **Förtydligad lagstiftning** avseende principerna om öppenhet, uppgiftsminimering, adekvat skyddsnivå och bindande företagsbestämmelser skulle öka harmoniseringen och rättssäkerheten för enskilda och företag.

När det gäller tillsynen skulle meddelanden från kommissionens inte undanröja medlemsstaternas motvilja mot att ändra nationella bestämmelser för att ge dataskyddsmyndigheter större oberoende och harmoniserade befogenheter. Förbättrad samordning av artikel 29-gruppen och utbyten mellan dataskyddsmyndigheter skulle ha en positiv inverkan på ett mer enhetligt genomförande av bestämmelserna. **Kvarstående skillnader mellan nationella lagar och mellan tolkningar av dessa skulle emellertid begränsa effekten av ett förbättrat samarbete mellan dataskyddsmyndigheter.**

De förväntade **finansiella och ekonomiska konsekvenserna av detta alternativ är begränsade**, och de konstaterade problemen skulle i stort sett förbli olösta.

6.2. Alternativ 2: En moderniserad rättslig ram

Rättsosäkerheten för privata företag och offentliga myndigheter **kommer att minskas avsevärt**. Problematiska bestämmelser kommer att förtydligas och enhetligheten kommer att förbättras till följd av det minskade tolkningsutrymmet och till följd av genomförandeåtgärder och/eller delegerade akter som antas av kommissionen.

Genom att den allmänna anmälan av uppgiftsbehandling ersätts med ett förenklat **harmoniserat "registreringssystem"**, samtidigt som man behåller förhandskontroller för känsliga uppgifter och för behandling som medför risker, befrias registeransvariga från en

skyldighet som för närvarande genomförs på olika sätt. Ett starkt ansvar för registeransvariga och registerförare genom införande av – i vissa fall och med tydligt definierade och bestämda tröskelvärden – uppgiftsskyddsombud och konsekvensbedömningar avseende uppgiftsskydd, och genom införande av principen om inbyggt uppgiftsskydd, kommer att göra det lättare att säkerställa och påvisa efterlevnaden av reglerna.

Preciseringar och förenklingar av bestämmelserna – en enda lag för hela EU och en enda kontaktpunkt för tillsyn över uppgiftsskyddet – kommer att stärka den inre marknaden bland annat genom att skillnaderna undanröjas i dataskyddsmyndigheternas administrativa formaliteter. Enbart vad gäller administrativa bördor kommer detta att göra det möjligt **sammanlagt spara ca 2,3 miljarder euro** per år.

Enhetligt genomförande främjas också genom att dataskyddsmyndigheternas befogenheter stärks och harmoniseras och genom att ett starkt samarbete skapas och en mekanism för ömsesidigt bistånd för fall som har en EU-dimension, och genom att en harmonisering sker av vilka överträdelser som omfattas av administrativa sanktioner.

En **EU-omfattande harmoniserad skyldighet att anmäla uppgiftsbrott** kommer att innebära att enskilda personer får bättre skydd, att enhetlighet mellan sektorer säkerställs och att konkurrenssnackdelar undviks.

Registrerades rättigheter och enskilda personers kontroll över sina egna uppgifter skulle stärkas betydligt genom införande av nya rättigheter samt genom att nuvarande rättigheter förbättras och ytterligare preciseras. Barn kommer att gynnas av åtgärder som specifikt tar hänsyn till deras sårbarhet. Sammanslutningar kommer att få större möjligheter att stödja registrerade när de utövar sina rättigheter, också inför domstol.

Tillämpningen av allmänna principer för uppgiftsskydd på området för polissamarbete och straffrättsligt samarbete skulle förbättra den övergripande enhetligheten i EU:s dataskyddslagstiftning samtidigt som hänsyn tas till brottsbekämpningens inneboende särdrag. Enskilda personers rättigheter skulle särskilt stärkas genom att tillämpningsområdet för uppgiftsskyddsbestämmelser på detta område utvidgas så att det även omfattar ”inhemsk” behandling, genom att villkor fastställs för att säkerställa rätten till tillträde och genom striktare regler om avgränsning av syfte.

När det gäller **finansiella och ekonomiska konsekvenser** kommer skyldigheten för större ekonomiska aktörer (mer än 250 anställda) att utse uppgiftsskyddsombud inte att **skapa oproportionerliga kostnader**, eftersom uppgiftsskyddsombud redan är vanligt förekommande i dessa företag. Kostnaderna för efterlevnaden av reglerna skulle uppgå till 320 miljoner euro per år. Skyldigheten skulle omfatta ett nödvändigt minimisegment av registeransvariga, eftersom små och medelstora företag som regel skulle vara undantagna från denna skyldighet, såvida inte deras uppgiftsbehandling medför betydande uppgiftsskyddsrisiker. Offentliga myndigheter och organ skulle få möjlighet att utse ett enda uppgiftsskyddsombud för flera enheter (t.ex. för flera filialer, avdelningar, kontor), med beaktande av deras organisatoriska struktur.

Förenklingar av bestämmelserna för internationella överföringar (t.ex. genom att utvidga tillämpningsområdet för ”bindande företagsbestämmelser”) skulle också ha en positiv inverkan på EU-företags internationella konkurrenskraft.

En förstärkning av dataskyddsmyndigheternas oberoende och befogenheter, tillsammans med medlemsstaternas skyldighet att förse dem med tillräckliga resurser, skulle medföra ytterligare kostnader för myndigheter som för närvarande inte har lämpliga befogenheter och tillräckliga resurser.

Det nya samarbetet och mekanismen för ömsesidigt bistånd mellan dataskyddsmyndigheter skulle också medföra ytterligare kostnader för nationella dataskyddsmyndigheter och Europeiska datatillsynsmannen. Exempelvis är det sannolikt att de ytterligare arbetsuppgifter som Europeiska datatillsynsmannen får för att tillhandahålla sekretariatet för Europeiska dataskyddsstyrelsen – som ersätter artikel 29-gruppen – och särskilt för sin medverkan i mekanismen för enhetlighet, kommer att kräva en ökning av dess nuvarande resurser med ytterligare 3 miljoner euro per år i genomsnitt under de första sex åren, inbegripet medel för ytterligare 10 tjänster.

6.3. Alternativ 3: Detaljerad lagstiftning på EU-nivå

Om ytterligare detaljerade bestämmelser, även sektorsspecifika, läggs till utöver åtgärderna enligt alternativ 2, skulle detta **minska skillnaderna mellan medlemsstaterna maximalt**. Eventuellt får medlemsstaterna emellertid då inte tillräckligt utrymme för att kunna ta hänsyn till nationella särdrag.

Avskaffas anmälningar helt – utom i samband med förhandskontroller – förenklas lagstiftningen avsevärt och administrationen minskar.

Inrättas en dataskyddsstyrelse på EU-nivå skulle **tillsynen bli mycket enhetligare** och bristande samstämmighet åtgärdas i fall med en klar EU-dimension, men en sådan styrelses befogenheter skulle kunna vara alltför vittgående för EU-lagstiftningen. Detta skulle dock vara mycket kostsamt för EU:s budget. Harmoniserade straffrättsliga påföljder skulle också bidra till en enhetlig tillsyn, men skulle också vara förenade med ett kraftigt motstånd från medlemsstaternas sida.

De registrerades rättigheter, inte minst barns rättigheter, skulle stärkas ytterligare, t.ex. genom att definitionen av känsliga uppgifter utvidgas till att även omfatta personuppgifter om barn samt biometriska och finansiella uppgifter. Införandet av en rätt till kollektiv talan skulle innebära att rättigheterna kan maximeras genom rättsprocesser. En EU-harmonisering av nivån vad gäller påföljder, bl.a. straffrättsliga påföljder, skulle stärka enskildas rättigheter ytterligare.

Konkreta ändringar av alla instrument så att de allmänna uppgiftsskyddsbestämmelserna även omfattar området för polissamarbete och straffrättsligt samarbete skulle inverka positivt på bestämmelsernas enhetlighet på detta område och stärka enskildas rättigheter. Ett sådant radikalt tillvägagångssätt skulle dock stöta på motstånd från medlemsstaternas sida och vara svårt att driva igenom politiskt.

7. JÄMFÖRELSE AV ALTERNATIVEN

Alternativ 1 skulle innebära låga kostnader för regelefterlevnad och administration, särskilt för privata registeransvariga, eftersom den största delen av merkostnaderna skulle bäras av nationella myndigheter och EU-myndigheter. Samtidigt skulle detta alternativ ha en **begränsad positiv inverkan på de problem som identifierats och de uppställda politiska målen**.

När det gäller i vilken utsträckning detta alternativ är politiskt genomförbart skulle det, även om förslagen nu inte är kontroversiella, sannolikt mötas av motstånd bland berörda parter därför att det bara i begränsad omfattning löser problemen. Det skulle inte heller betraktas som tillräckligt ambitiöst.

Alternativ 2 kommer att leda till att **fragmentering och rättsosäkerhet minskar avsevärt**. Det förväntas i mycket högre grad lösa de identifierade problemen och bidra till att de politiska målen uppfylls. **De kostnader för efterlevnad och administration som är förknippade med detta alternativ väntas bli rimliga mot bakgrund av den nytta som åstadkoms och besparingarna för administration på omkring 2,3 miljarder euro per år. Detta är mycket viktigt för företagen.** Detta alternativ kommer att säkerställa en bättre och mer enhetlig tillsyn totalt sett. Om anmälningar avskaffas och ett mycket enklare system med basregistrering införs skulle detta även förenkla lagstiftningen och minska den administrativa bördan.

När det gäller berörda parter acceptans torde detta alternativ generellt sett mottas positivt av de ekonomiska aktörerna och offentliga myndigheter, eftersom det skulle minska deras kostnader för efterlevnaden av reglerna, särskilt de kostnader som uppstår på grund av de nuvarande disparata bestämmelserna. Alla som arbetar med uppgiftsskydd och inte minst dataskyddsmyndigheterna skulle välkomna ett förstärkt uppgiftsskydd. Vad beträffar det tredje allmänna målet skulle detta alternativ bidra till att uppfylla målet om att se till att uppgiftsskyddsbestämmelserna blir mer **samstämmiga och enhetliga på området polissamarbete och straffrättsligt samarbete** genom att rambeslutet upphävs och uppdateras i överensstämmelse med Lissabonfördraget, så att bristerna i detta åtgärdas, i synnerhet genom att tillämpningsområdet utvidgas till att omfatta "inhemsk" behandling.

Alternativ 3 innehåller de flesta av de åtgärder som ingår i alternativ 2, men är på flera punkter mer omfattande. Det skulle därför få **stor och positiv inverkan när det gäller både att minska de kostnader som är förknippade med den fragmenterade lagstiftningen och att stärka enskildas rättigheter**. Det skulle dessutom maximera enhetligheten i fråga om uppgiftsskyddsbestämmelserna inom den tidigare tredje pelaren och höja standarderna för uppgiftsskydd på det området. Vissa åtgärder som ingår i detta alternativ är dock antingen förknippade med **alltför höga kostnader för regelefterlevnaden eller kommer sannolikt att stöta på stort motstånd från berörda parter sida**. Det skulle dessutom bli mycket komplicerat och vara politiskt kontroversiellt att samtidigt ändra alla instrument inom den tidigare tredje pelaren.

Rekommenderat alternativ

Det **alternativ som föredras** är alternativ 2 kombinerat med

- att anmälningsplikten avskaffas så som anges i alternativ 3, och
- att vissa "mjuka" åtgärder från alternativ 1 vidtas, nämligen att integritetsfrämjande teknik och certifieringssystem uppmuntras och att medvetandehöjande kampanjer genomförs.

Med det rekommenderade alternativet är det mest sannolikt att de politiska mål som ställts upp uppnås utan alltför höga kostnader för regelefterlevnaden, samtidigt som den administrativa bördan minskar betydligt.

De skärpta uppgiftsskyddsbestämmelserna väntas leda till vissa ytterligare kostnader för efterlevnaden av reglerna, i synnerhet för registeransvariga som har hand om uppgiftsbehandling som medför risker. Ett starkt uppgiftsskydd kan dock innebära en konkurrensfördel för EU:s ekonomi, eftersom ett starkt skydd och det förhållandet att antalet överträdelser av uppgiftsskyddet väntas minska kan öka konsumenternas förtroende. Om företagen måste uppfylla höga krav på uppgiftsskydd kan detta även leda till långsiktiga förbättringar för de europeiska företagen, som kan bli världsledande inom integritetsfrämjande teknik och lösningar för inbyggt integritetsskydd, vilket kan locka företag, arbetstillfällen och kapital till EU.

För företag som bedriver verksamhet på EU:s inre marknad kommer den ökade harmoniseringen dessutom att leda till att gränsöverskridande behandling av personuppgifter blir enklare och billigare. Dessa företag väntas därigenom få avsevärda incitament att expandera över gränserna och dra nytta av de fördelar som den inre marknaden innebär, vilket både konsumenterna och den europeiska ekonomin som helhet vinner på.

Det rekommenderade alternativet utgör en balanserad lösning även på problem 3, eftersom det innebär att enskildas rättigheter stärks, brister åtgärdas och den bristande enhetligheten minskar när det gäller uppgiftsskydd på området polissamarbete och straffrättsligt samarbete, samtidigt som tillsynsmyndigheternas samarbete underlättas och sektorns särdrag och operativa behov respekteras.

8. ÖVERVAKNING OCH UTVÄRDERING

Övervakningen och utvärderingen av konsekvenserna av det rekommenderade alternativet kommer att inriktas på aspekter som t.ex. användningen av de nya instrument som införs genom reformen, de nationella dataskyddsmyndigheternas befogenheter och resurser, påföljder som utdöms för överträdelser av dataskyddslagstiftningen, de registeransvarigas kostnader för regelefterlevnaden och den tid de måste lägga på detta samt utvecklingen av de enskildas förtroende för skyddet av deras personuppgifter på internet.