EUROPEISKA KOMMISSIONEN

Bryssel den 4.11.2010
KOM(2010) 609 slutlig

KOMMISSIONENS MEDDELANDE TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN OCH REGIONKOMMITTÉN

Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen

KOMMISSIONENS MEDDELANDE TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN OCH REGIONKOMMITTÉN

Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen

1. NYA UTMANINGAR I FRÅGA OM SKYDDET AV PERSONUPPGIFTER

Direktivet om skydd av personuppgifter[1] från 1995 innebar ett stort framsteg för skyddet av personuppgifter i Europeiska unionen. Direktivet fastställer två av de äldsta och viktigaste målen för den europeiska integrationen, nämligen skyddet av de grundläggande fri- och rättigheterna och i synnerhet skyddet av personuppgifter å ena sidan samt inrättandet av den inre marknaden med bland annat ett fritt flöde av personuppgifter å den andra.

Ännu femton år senare är denna dubbla målsättning aktuell och de principer som stadfästes i direktivet har inte förlorat sitt berättigande. **Men den snabba tekniska utvecklingen och globaliseringen har förändrat omvärlden i grunden och medfört nya utmaningar för skyddet av personuppgifter.**

Med dagens teknik kan enskilda på ett tidigare otänkbart sätt enkelt dela information om sina vanor och preferenser offentligt och globalt. Det kanske mest uppenbara exemplet är webbplatser för sociala nätverk med hundratals miljoner medlemmar över hela världen, men det är inte det enda. Datormoln – dvs. Internetbaserade tjänster där programvara, delade resurser och information läggs på externa servrar (i molnet) kan också vara problematiska för skyddet av personuppgifter, eftersom individerna tappar kontrollen över potentiellt känsliga uppgifter när de lagras i program på någon annans hårdvara. En färsk undersökning bekräftar att myndigheter med ansvar för skyddet av personuppgifter, företagsorganisationer och konsumentföreningar alla tycks anse att onlineverksamheten idag innebär ökade risker för den personliga integriteten och skyddet av personuppgifter.[2]

Samtidigt **samlas personuppgifter in med allt mer sofistikerade metoder som är svårare att spåra.** Avancerade verktyg ger till exempel ekonomiska aktörer mer information om enskildas beteenden, som de sedan kan använda i sina riktade kontakter. Och den ökande användningen av automatisk uppgiftsinsamling vid utfärdande av elektroniska biljetter, vägtullar eller för gps-system gör det lättare att se var enskilda personer befinner sig när de använder mobila apparater. Myndigheterna använder också personuppgifter på allt fler sätt, till exempel för att spåra personer vid epidemier, för att mer effektivt förebygga eller bekämpa terrorism och annan brottslighet, för förvaltningen av sociala trygghetssystem, i beskattningssyften, i programvara för den digitala förvaltningen osv.

---

1 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).

2 Se undersökningen *Study on the economic benefits of privacy enhancing technologies*, London Economics, juli 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), s. 14.

Allt detta väcker förstås frågan om EU:s nuvarande bestämmelser om skydd av personuppgifter fortfarande räcker till för att hantera dessa utmaningar på ett effektivt sätt.

För att utreda frågan inledde kommissionen en översyn av gällande bestämmelser genom en högnivåkonferens i maj 2009, som sedan följdes upp av ett offentligt samråd vars remisstid gick ut i slutet av år 2009.[3] Samtidigt inleddes flera undersökningar.[4]

Svaren bekräftade att de grundläggande principerna i direktivet fortfarande är giltiga och att den tekniskt neutrala karaktären bör bevaras. Däremot belystes flera frågor som kunde ge upphov till särskilda problem. Dessa redovisas nedan.

- *Hantera konsekvenserna av den nya tekniken*

Remissvaren, både från enskilda och från organisationer, bekräftar att man bör förtydliga och precisera hur principerna om skydd av personuppgifter ska tillämpas på ny teknik, för att se till att enskildas personuppgifter får ett faktiskt och effektivt skydd, oavsett vilken teknik som används för att behandla uppgifterna, och för att se till att de registeransvariga är fullt medvetna om hur den nya tekniken påverkar skyddet av personuppgifter. Detta har delvis reglerats genom direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation)[5] som detaljerar och kompletterar det allmänna direktivet om skydd av personuppgifter, med avseende på elektronisk kommunikation.[6]

- *Stärka inremarknadsaspekten på skyddet av personuppgifter*

Ett återkommande bekymmer för aktörerna, i synnerhet multinationella företag, är bristen på harmonisering mellan medlemsstaternas lagstiftning om skydd av personuppgifter trots att det finns en gemensam rättslig ram på EU-nivå. Företagen framhöll att rättssäkerheten bör öka, byråkratin minska och ekonomiska aktörer och andra registeransvariga ges likvärdiga förutsättningar.

---

3 Se svaren på kommissionens offentliga samråd: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Riktade remisser till vissa aktörer gjordes under 2010. Kommissionens vice ordförande Viviane Reding höll även ett högnivåmöte med aktörer den 5 oktober 2010 i Bryssel. Kommissionen hörde också arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (den s.k. artikel 29-gruppen) som lämnade ett uttömmande svar på samrådet 2009 (WP 168) och i juli 2010 antog ett särskilt yttrande om ansvarsfrågorna (WP 173).

4 Utöver undersökningen *Study on the Economic Benefits of Privacy Enhancing Technologies* (som citerades i fotnot 2) se även undersökningen *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments* från januari 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). En annan undersökning pågår just nu med anledning av konsekvensbedömningen av EU:s framtida lagstiftning om skydd av personuppgifter.

5 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), (EGT L 201, 31.7.2002, s. 37).

6 I direktivet om skydd av personuppgifter 95/46/EG fastställs normer för skydd av personuppgifter avseende alla EU:s rättsakter, däribland direktivet om integritet och elektronisk kommunikation 2002/58/EG (ändrat av direktiv 2009/136/EG, EUT L 337, 18.12.2009, s. 11). Direktivet om integritet och elektronisk kommunikation är tillämpligt på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen. Det överförde principerna i direktivet om skydd av personuppgifter till särskilda bestämmelser om elektroniska kommunikationstjänster. Direktiv 95/46/EG är bland annat tillämpligt på privata kommunikationstjänster.

- *Hantera globaliseringen och förbättra den internationella överföringen av uppgifter*

Flera aktörer betonade att behandlingen allt oftare läggs ut på entreprenad, ofta utanför EU och att detta ger upphov till flera problem med avseende på vilken lag som ska tillämpas på behandlingen och hur det därmed sammanhängande ansvaret fördelas. Vid internationell överföring av uppgifter anser många organisationer att dagens system inte är helt tillfredsställande utan att de bör ses över och rationaliseras för att göra överföringarna enklare och mindre omständliga.

- *Stärka de institutioner som ska tillämpa bestämmelserna om skydd av personuppgifter*

Aktörerna är ense om att de myndigheter som ansvarar för skyddet av personuppgifter bör få ett starkare inflytande för att kunna verkställa bestämmelserna om skydd av personuppgifter på ett bättre sätt.[7] Vissa organisationer efterlyste också ökad insyn i det arbete som bedrivs i artikel 29-gruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (*se 2.5. nedan*) och ett förtydligande av gruppens uppgifter och behörighet.

- *Göra regelverket för skyddet av personuppgifter mer enhetligt*

Vid det offentliga samrådet betonade alla aktörer behovet av ett övergripande instrument som är tillämpligt på behandlingen av personuppgifter på alla EU:s sektorer och politikområden så att man hanterar frågan på ett sammanhängande och smidigt sätt och därmed garanterar ett kontinuerligt och verkningsfullt skydd.

Dessa utmaningar **kräver att EU utvecklar ett samlat och konsekvent grepp** för att se till att **enskildas grundläggande rätt till skydd av personuppgifter efterlevs till fullo såväl inom som utanför EU**. Lissabonfördraget ger EU möjligheter att genomföra detta i och med att EU: stadga om de grundläggande rättigheterna blev rättsligt bindande. I stadgans artikel 8 införs en fristående rätt till skydd av personuppgifter. Samtidigt infördes en ny rättslig grund[8] som gör det möjligt att utarbeta en omfattande och konsekvent EU-lagstiftning om skydd av enskilda när det gäller behandling av personuppgifter och om det fria flödet av sådana uppgifter. Den nya rättsliga grunden ger i synnerhet EU möjligheter att anta en enda rättsakt om skydd av personuppgifter, som även omfattar polissamarbete och samarbete i straffrättsliga frågor (polisiärt och straffrättsligt samarbete). Den gemensamma utrikes- och säkerhetspolitiken täcks endast delvis av artikel 16 i EU-fördraget, eftersom särskilda bestämmelser om medlemsstaternas behandling av personuppgifter måste fastställas i ett beslut från rådet, som ska antas enligt en annan rättslig grund.[9]

Mot bakgrund av dessa nya juridiska möjligheter kommer kommissionen att ge högsta prioritet åt respekten för den grundläggande rätten till skydd av personuppgifter inom hela EU och på alla politikområden, samtidigt som inremarknadsaspekten och det fria flödet av dessa uppgifter stärks. Man måste i sammanhanget också ta hänsyn till andra relevanta

---

7 I enskilda svar som lämnades efter det att den officiella remisstiden löpt ut anförde Europol och Eurojust att man icke desto mindre måtte ta hänsyn till den särskilda karaktären på deras verksamhet när det gäller samordning av rättstillämpande instanser och brottsförebyggande åtgärder.

8 Se artikel 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

9 Se artikel 16.2 sista stycket i EUF-fördraget och artikel 39 i fördraget om Europeiska unionen (EU-fördraget).

grundläggande rättigheter i stadgan och andra mål i fördragen, samtidigt som man garanterar den grundläggande rätten till skydd av personuppgifter.

Det här meddelandet beskriver hur kommissionen ska modernisera EU:s rättsliga ram för skyddet av personuppgifter på alla EU:s verksamhetsområden, med särskild hänsyn till de utmaningar som globaliseringen och den nya tekniken medför, för att garantera enskilda ett gott skydd i samband med behandling av personuppgifter på alla EU:s verksamhetsområden. Därmed kan EU driva på de internationella normerna för skydd av personuppgifter.

2. HUVUDSAKLIGA MÅLSÄTTNINGAR FÖR ETT SAMLAT GREPP PÅ SKYDDET AV PERSONUPPGIFTER

2.1. Stärka enskildas rättigheter

2.1.1. Garantera enskilda lämpligt skydd i alla situationer

Syftet med bestämmelserna i EU:s nuvarande lagstiftning om skydd av personuppgifter är **att skydda fysiska personers grundläggande fri- och rättigheter och i synnerhet rätten till skydd av personuppgifter**, i enlighet med EU:s stadga om de grundläggande rättigheterna.[10]

Begreppet personuppgifter är centralt för skyddet av enskilda enligt EU:s gällande bestämmelser om skydd av personuppgifter och medför skyldigheter för registeransvariga och registerförare.[11] Definitionen av begreppet personuppgifter syftar till att inbegripa varje upplysning som avser en identifierad eller direkt eller indirekt identifierbar fysisk person. För att avgöra om en person är identifierbar ska man beakta ”alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person”[12]. Den metod lagstiftaren valt har fördelen att den är flexibel och kan anpassas till olika situationer och utvecklingar som påverkar de grundläggande rättigheterna, även sådana som inte kunde förutses när direktivet antogs. Men konsekvenserna av denna breda och flexibla formulering är också att det i många fall inte står helt klart om direktivet är tillämpligt, om enskildas personuppgifter är skyddade och vilka registeransvariga som är bundna av skyldigheterna enligt direktivet.[13]

Vissa situationer där särskilda uppgifter behandlas skulle kräva ytterligare lagstiftningsåtgärder på EU-nivå. I vissa fall har sådana åtgärder redan vidtagits. Lagring av uppgifter i terminaler (som exempelvis mobiltelefoner) är till exempel bara tillåten med samtycke från de berörda. Dessa fall kan också kräva insatser på EU-nivå, till exempel när det gäller kodade uppgifter, lokaliseringsuppgifter, teknik för datautvinning som gör det möjligt

---

10 Se EG-domstolens dom i mål C-101/01, Bodil Lindqvist, (REG 2003, s. I-1297) punkterna 96, 97 samt mål C-275/06, Productores de Música de España (Promusicae) mot Telefónica de España SAU, (REG 2008, s. I-271). Se även rättspraxis från Europeiska domstolen för de mänskliga rättigheterna, t.ex. mål S. and Marper mot Förenade kungariket, 4.12.2008 (Application nos. 30562/04 and 30566/04) och Rotaru mot Rumänien, 4.5. 2000, nr. 28341/95, § 55, ECHR 2000-V.

11 Se definitionerna av ”registeransvarig” och ”registerförare” i artikel 2d och 2e i direktiv 95/46/EG.

12 Se skäl 26 i direktiv 95/46/EG.

13 Se till exempel frågan om IP-adresser, som tas upp i yttrande 4/2007 från artikel 29-gruppen avseende personuppgifter (WP 136).

att kombinera uppgifter från olika källor eller när man måste garantera IT-systemens säkerhet och integritet[14].

Alla dessa frågor bör därför noggrant utredas.

Kommissionen kommer att överväga **hur man kan garantera en konsekvent tillämpning av bestämmelserna om skydd av personuppgifter, med hänsyn till hur den nya tekniken påverkar enskildas fri- och rättigheter i syfte att garantera den fria rörligheten för personuppgifter på den inre marknaden**.

2.1.2. Öka de registrerades insyn

Insyn är grundläggande för att individerna ska kunna kontrollera sina egna uppgifter och för att personuppgifterna ska få ett effektivt skydd. Det är därför mycket viktigt att de registeransvariga informerar enskilda **på ett uttömmande och tydligt sätt** om hur och varför personuppgifter samlas in och behandlas, i vilka syften, hur lång tid uppgifterna lagras och vilka rättigheter de registrerade har att få tillgång till, korrigera eller utplåna uppgifterna. De relevanta bestämmelserna om information till de registrerade[15] är otillräckliga.

Grundläggande är krav på att **informationen ska vara lättillgänglig och lättförståelig och att ett klart och enkelt språk används**. Detta är särskilt viktigt online, där meddelanden om skydd av personuppgifter ofta är otydliga, svårtillgängliga eller icke insynsvänliga[16] och dessutom inte alltid följer gällande bestämmelser. Ett exempel är beteendestyrd annonsering online, där de många aktörer som står bakom annonseringen och teknikens komplexitet gör det svårt för enskilda att veta och förstå om personuppgifter samlas in, av vem och i vilket syfte.

I detta sammanhang måste **barn** få särskilt skydd, eftersom de inte är lika medvetna om hur behandlingen av personuppgifter påverkar risker, följder, skydd och rättigheter[17].

Kommissionen kommer att överväga att

- införa en **allmän princip om insynsvänlig behandling** av personuppgifter inom den rättsliga ramen,

- införa **särskilda skyldigheter** för registeransvariga när det gäller vilken sorts information som lämnas och **hur** den lämnas, däribland information som riktar sig till **barn,**

- utarbeta ett eller flera **standardformulär** (”**meddelande om skydd av personuppgifter**”) som ska användas av de registeransvariga **inom EU**.

---

14 Se till exempel domen från den tyska Bundesverfassungsgericht av den 27 februari 2008, 1 BvR 370/07.

15 Se artiklarna 10 och 11 i direktiv 95/46/EG.

16 I en Eurobarometerundersökning från 2009 framkom att ungefär hälften av de tillfrågade ansåg att meddelandena om skydd av personuppgifter på webbplatser var ”mycket” eller ”ganska” oklara (Flash Eurobarometer nr 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

17 Se undersökningen om säkrare Internet för barn i åldrarna 9–10 och 12–14 som visade att barnen tenderar att underkatta de risker som är förknippade med Internetanvändning och att minimera konsekvenserna av riskbeteenden : (http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

Det är också viktigt att enskilda informeras ifall deras uppgifter oavsiktligt eller uppsåtligt förstörs, förloras, ändras, läses av eller lämnas ut till obehöriga. Efter en översyn nyligen av direktivet om integritet och elektronisk kommunikation infördes en **obligatorisk anmälan av personuppgiftsbrott** som dock enbart omfattar telekommunikationer. Eftersom risken för sådana brott även föreligger på andra områden (till exempel den finansiella sektorn), kommer kommissionen att undersöka möjligheterna att utvidga anmälningsplikten av personuppgiftsbrott till att även omfatta andra sektorer, i enlighet med kommissionens uttalande om anmälan av personuppgiftsbrott inför Europaparlamentet 2009 i samband med översynen av den rättsliga ramen för elektronisk kommunikation.[18] Kommissionens undersökning ska inte påverka bestämmelserna i direktivet om integritet och elektronisk kommunikation, som ska införlivas med nationell lagstiftning senast den 25 maj 2011.[19] Det är viktigt att frågan behandlas enhetligt och konsekvent.

Kommissionen kommer att

- undersöka hur man inom den allmänna rättsliga ramen skulle kunna ta in allmänna bestämmelser om **anmälan av personuppgiftsbrott**, inklusive bestämmelser om till vilka anmälan ska riktas och vilka omständigheter som ska utlösa anmälningsskyldigheten.

2.1.3. Förbättra kontrollen över de egna uppgifterna

Två viktiga förutsättningar för att garantera enskilda ett gott uppgiftsskydd är **att de registeransvarigas behandling begränsas till vissa syften (dataminimering)** och att den registrerade behåller en **faktisk kontroll över sina egna uppgifter**. I artikel 8.2 i stadgan sägs: ”Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem”. Enskilda bör alltid kunna få tillgång till, korrigera, utplåna eller blockera sina uppgifter om det inte i lag finns välmotiverade skäl som talar mot detta. Dessa rättigheter föreligger redan enligt den nuvarande rättsliga ramen. Däremot har man inte harmoniserat hur rättigheterna utövas, och därför är det lättare att åberopa sina rättigheter i vissa medlemsstater än i andra. Dessutom har detta lett till särskilda utmaningar online, där uppgifterna ofta lagras utan att den berörda personen informeras eller har lämnat sitt samtycke.

Ett särskilt tydligt exempel är sociala nätverk online som innebär särskilda utmaningar för individernas faktiska kontroll över sina personuppgifter. Kommissionen har fått flera frågor från personer som inte kunnat dra tillbaka personlig information, till exempel foton, från tjänsteleverantörer online, vilket inneburit en kränkning av deras rätt att få tillgång till, korrigera och utplåna uppgifter.

Dessa rättigheter bör därför göras mer uttryckliga, förtydligas och om möjligt stärkas.

---

[18] ”Kommissionen noterar Europaparlamentets önskan att en skyldighet att meddela personuppgiftsöverträdelser inte ska begränsas till sektorn för elektronisk kommunikation utan också gälla aktörer såsom leverantörer av informationssamhällets tjänster […]. Kommissionen kommer därför att utan dröjsmål inleda ett lämpligt förberedande arbete som inkluderar samråd med intressenter, med syfte att lägga fram förslag inom detta område senast 2011 i enlighet med behoven […]”, se http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN. Se även skäl 59 i direktiv 2009/136/EG om ändring av direktivet om integritet och elektronisk kommunikation 2002/58/EG: ”Det är inte bara inom sektorn för elektronisk kommunikation som användarna har ett allmänintresse av att informeras och därför bör det vara en prioriterad målsättning att på gemenskapsnivå införa obligatoriska anmälningskrav inom alla sektorer.”

[19] Artikel 4 i direktiv 2009/136/EG.

Kommissionen kommer därför att undersöka olika möjligheter att

- skärpa **principen om att behandling bara får ske i vissa syften (dataminimering),**

- **förbättra villkoren** för det faktiska **utövandet av rätten att få tillgång till, korrigera, utplåna eller blockera uppgifter** (t.ex. genom att införa frister för att besvara förfrågningar från enskilda, göra det möjligt att utöva sina rättigheter elektroniskt eller genom att fastställa att tillgången till personuppgifter i princip bör vara gratis),

- förtydliga **rätten till radering**, dvs. enskildas rätt att begära att behandlingen av personuppgifterna upphör och att de raderas när de inte längre behövs av legitima skäl, till exempel när behandlingen skett med personens samtycke och detta samtycke återkallats eller när den tillåtna lagringstiden löpt ut,

- komplettera de registrerades rättigheter genom att garantera **uppgifternas portabilitet**, dvs. en uttrycklig rätt för enskilda att återkalla uppgifter (foton, listor över vänner o.dyl.) från ett program eller en tjänst så att de återkallade uppgifterna kan överföras till ett annat program eller en annan tjänst i den mån detta är tekniskt möjligt, utan hinder av de registeransvariga.

2.1.4. Öka medvetenheten

Insyn är viktigt men man bör också göra allmänheten, och i synnerhet ungdomar, mer medvetna om sina rättigheter och de risker som är förknippade med behandlingen av personuppgifter. Enligt en Eurobarometerundersökning från 2008 anser en bred majoritet i EU:s medlemsstater att medvetenheten om skyddet av personuppgifter är låg i deras land.[20] Därför bör medvetandegörande åtgärder vidtas och främjas av en rad aktörer, däribland myndigheter i medlemsstaterna, i synnerhet myndigheter med ansvar för skyddet av personuppgifter och utbildningsorgan, vid sidan av registeransvariga och frivilligorganisationer. Åtgärderna bör avse annat än lagstiftning, till exempel informationskampanjer i press och elektroniska medier samt presentation av klar och tydlig information på webbplatser med tydligt angivande av de registrerades rättigheter och de registeransvarigas ansvar.

Kommissionen kommer att undersöka

- möjligheten att via EU:s budget **samfinansiera medvetandegörande åtgärder avseende skydd av personuppgifter**,

- behovet av och lämpligheten i att i den rättsliga ramen ta in **en skyldighet att vidta medvetandegörande åtgärder** på området.

2.1.5. Kräva välinformerade och frivilliga samtycken

När det krävs samtycke för att kunna behandla personuppgifter avser detta enligt gällande bestämmelser en ”frivillig, särskild och informerad viljeyttring”, genom vilken den registrerade godtar behandling av personuppgifter som rör honom eller henne[21]. Men dessa villkor tolkas idag på olika sätt av medlemsstaterna, där villkoren spänner över allt mellan skriftligt samtycke och att godta underförstådda samtycken.

---

[20] Se Flash Eurobarometer nr 225 – Data Protection in the European Union: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Se artikel 2h i direktiv 95/46/EG.

Den bristande öppenheten i policyn för integritetsskydd gör att enskilda online ofta har svårt att få reda på sina rättigheter och lämna välinformerade samtycken. Detta försvåras ytterligare av att det i vissa fall inte ens framgår hur ett frivilligt, särskilt och informerat samtycke till behandling av personuppgifter borde vara utformat, till exempel när det gäller beteendestyrd annonsering, där webbläsarinställningarna av vissa, men inte av andra, anses utgöra samtycke från användaren.

Därför bör villkoren för samtycke från de registrerade förtydligas, så att samtycke alltid lämnas av välinformerade individer som är fullt medvetna om att de lämnar sitt samtycke och vilken behandling de medgivit, i enlighet med artikel 8 i EU:s stadga om de grundläggande rättigheterna. Tydliga nyckelbegrepp kan också göra det lättare att utveckla självreglering för att ta fram praktiska lösningar som är förenliga med EU-lagstiftningen

Kommissionen kommer att undersöka hur man skulle kunna **förtydliga och skärpa bestämmelserna om samtycke**.

2.1.6. Skydda känsliga uppgifter

Det är idag generellt förbjudet att behandla känsliga uppgifter, till exempel personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv, med begränsade undantag på vissa villkor och enligt vissa garantier.[22] Mot bakgrund av den tekniska och samhälleliga utvecklingen bör man dock se över de befintliga bestämmelserna om känsliga uppgifter för att se om andra kategorier av uppgifter bör läggas till och för att ytterligare förtydliga villkoren för behandling. Detta gäller till exempel genetiska uppgifter som idag inte ingår i kategorin känsliga uppgifter.

Kommissionen kommer att överväga

- om olika kategorier av uppgifter bör anses utgöra ”**känsliga uppgifter**”, till exempel **genetiska** uppgifter,

- om man ytterligare bör förtydliga och **harmonisera villkoren** för behandling av uppgiftskategorier som är känsliga.

2.1.7. Göra rättsmedel och påföljder mer verkningsfulla

Skyddet av personuppgifter kräver **verkningsfulla bestämmelser om rättsmedel och påföljder**. När en person får problem därför att bestämmelserna om skyddet av personuppgifter överträtts befinner sig ofta många andra i samma situation.

Kommissionen kommer därför att

- överväga möjligheten att ge även myndigheter med ansvar för att skydda personuppgifter, frivilligorganisationer samt **andra sammanslutningar som företräder de registrerades intressen rätt att väcka talan vid nationell domstol,**

- bedöma behovet av **skärpta påföljder**, till exempel genom att uttryckligen inkludera även brottspåföljder vid allvarliga överträdelser av bestämmelserna om skydd av personuppgifter för att göra bestämmelserna mer verkningsfulla.

[22] Se artikel 8 i direktiv 95/46/EG.

2.2. Stärka inremarknadsaspekten

2.2.1. Öka rättssäkerheten och ge de registeransvariga likvärdiga förutsättningar

Skyddet av personuppgifter i EU har även en **stark inremarknadsaspekt**, dvs. det finns ett behov av att tillåta fri rörlighet för personuppgifter mellan medlemsstaterna inom den inre marknaden. Direktivets harmonisering av de nationella lagstiftningarna inskränker sig således inte till en minimiharmonisering, utan leder till en i princip fullständig harmonisering.[23]

Samtidigt ger direktivet medlemsstaterna handlingsutrymme på vissa områden och tillåter att de bibehåller eller inför särregleringar för specifika situationer.[24] Eftersom direktivet i vissa fall har genomförts felaktigt av medlemsstaterna har detta lett till **skillnader mellan de nationella genomförandebestämmelserna, vilket motverkar ett av direktivets huvudsyften, nämligen att säkerställa det fria flödet av personuppgifter inom den inre marknaden**. Detta gäller ett stort antal branscher och sammanhang, till exempel behandlingen av personuppgifter i arbetslivet eller i folkhälsosammanhang. Bristande harmonisering är ett stort återkommande problem som framhålls av privata aktörer, i synnerhet ekonomiska aktörer, eftersom det innebär merkostnader och extra byråkrati. Särskilt drabbas registeransvariga med säte i flera medlemsstater som måste följa alla krav och praxis i vart och ett av dessa länder. Att direktivet genomförts på olika sätt i olika medlemsstater undergräver rättsäkerheten inte bara för de registeransvariga utan även för de registrerade, och innebär en risk för snedvridning av det likvärdiga skydd som direktivet skulle införa och säkerställa.

Kommissionen kommer att undersöka möjligheterna till **ytterligare harmonisering av bestämmelserna om skydd av personuppgifter på EU-nivå**.

2.2.2. Minska byråkratin

Om likvärdiga förutsättningar föreligger behöver man inte längre ta hänsyn till olikartade nationella krav, vilket i sin tur väsentligt minskar byråkratin för de registeransvariga. **Att se över och förenkla dagens anmälningssystem**[25] skulle ytterligare minska byråkratin och sänka de registeransvarigas kostnader. Det finns en samsyn bland de registeransvariga om att det nuvarande allmänna anmälningskravet av all behandling till myndigheter med ansvar för skyddet av personuppgifter är relativt tungrott och inte förbättrar skyddet av personuppgifterna. I denna fråga har medlemsstaterna dessutom visst handlingsutrymme enligt direktivet, eftersom de själva kan besluta om eventuella undantag och förenklingar, samt om vilka förfaranden som ska följas.

Ett harmoniserat och förenklat system skulle minska både kostnaderna och byråkratin, i synnerhet för multinationella företag med säte i flera medlemsstater.

Kommissionen kommer att undersöka olika möjligheter att **förenkla och harmonisera dagens anmälningssystem**, till exempel med hjälp av **ett anmälningsformulär för hela EU**.

---

23 EG-domstolens dom i mål C-101/01, Bodil Lindqvist, (REG 2003, s. I-1297), punkterna 96 och 97.

24 *Ibidem*, punkt 97. Se även skäl 9 i direktiv 95/46/EG.

25 Se artikel 18 i direktiv 95/46/EG.

2.2.3. Förtydliga bestämmelserna om tillämplig lagstiftning och medlemsstaternas ansvar

Redan i kommissionens första rapport om genomförandet av direktivet om skydd av personuppgifter år 2003[26] betonades att bestämmelserna om tillämplig lagstiftning[27] genomförts ”bristfälligt, vilket resulterar i att det kan uppstå sådana typer av rättsliga konflikter som man genom denna artikel försökt undvika”. Situationen har inte förbättrats sedan dess, varför registeransvariga och tillsynsmyndigheter i medlemsstaterna inte alltid vet vilken medlemsstat som är ansvarig och vilken lag som är tillämplig när flera medlemsstater berörs. Det gäller i synnerhet när en registeransvarig är underställd olika krav från olika medlemsstater, när ett multinationellt företag har säte i mer än en medlemsstat och när den registeransvariga inte har säte i EU men erbjuder tjänster som riktar sig till personer bosatta i EU.

Globaliseringen och den tekniska utvecklingen gör också frågan mer komplex: det blir allt vanligare att registeransvariga är verksamma i flera medlemsstater och rättssystem samt att de tillhandahåller tjänster och hjälp dygnet runt. Internet gör det lättare för registeransvariga med säte utanför EES[28] att tillhandahålla tjänster på distans och behandla personuppgifter online och det är ofta svårt att avgöra var personuppgifter och den utrustning som används befinner sig (till exempel när program och tjänster anlitar datormoln).

Bara för att personuppgifterna behandlas av en registeransvarig med säte i tredjeland bör dock inte enskilda berövas den rätt till skydd de har enligt EU:s stadga om de grundläggande rättigheterna och enligt EU:s lagstiftning om skydd av personuppgifter.

Kommissionen kommer därför att utreda hur man kan **se över och förtydliga de befintliga bestämmelserna om tillämplig lagstiftning.** Detta skulle inbegripa en genomgång av lagvalsreglerna för att öka rättsäkerheten, förtydliga medlemsstaternas ansvar för tillämpningen av bestämmelserna om skydd av personuppgifter och för att nå en likvärdig skyddsnivå inom EU av de registrerades uppgifter, oavsett var den registeransvariga befinner sig.

2.2.4. Öka de registeransvarigas ansvar

Administrativ förenkling får **inte leda till att de registeransvarigas ansvar för skyddet av personuppgifter minskar**. Tvärtom anser kommissionen att ansvaret bör förtydligas i den rättsliga ramen, även med avseende på förhållandet till interna kontrollsystem och samarbete med tillsynsmyndigheter. Man bör vidare utvidga ansvaret även till registeransvariga med tystnadsplikt (t.ex. advokater) samt till de allt vanligare situationer där de registeransvariga delegerat behandlingen till andra.

Kommissionen kommer därför att undersöka hur man kan **se till att registeransvariga vidtar verkningsfulla åtgärder och inför system för att följa bestämmelserna om skydd av personuppgifter**. Kommissionen kommer därvid att ta hänsyn till den pågående debatten om ”accountability”[29]. Syftet är inte att öka byråkratin för de registeransvariga, utan åtgärderna inriktas på att inrätta garantier och system för att effektivisera efterlevnaden av

---

[26] Rapport från kommissionen – Första rapporten om genomförandet av dataskyddsdirektivet (95/46/EG), KOM(2003) 265 slutlig.

[27] Se artikel 4 i direktiv 95/46/EG.

[28] Europeiska ekonomiska samarbetsområdet omfattar Norge, Liechtenstein och Island.

[29] Se i synnerhet från artikel 29-gruppens yttrande 3/2010 av den 13 juli.

bestämmelserna om uppgiftsskydd, samtidigt som man minskar och förenklar vissa administrativa formaliteter som t.ex. anmälningsskyldigheten (*se 2.2.2 ovan*).

I sammanhanget kan det även för skyddet av personuppgifter vara lämpligt att främja användningen av integritetsfrämjande teknik, något som redan framhölls i kommissionens meddelande från 2007, samt inbyggda skyddsmekanismer för den personliga integriteten.[30]

Kommissionen kommer att utreda följande för att öka de registeransvarigas ansvar:

– Göra det obligatoriskt att utse ett oberoende **uppgiftsskyddsombud** och harmonisera bestämmelserna om deras uppdrag och behörighet[31] och samtidigt överväga lämpliga gränsdragningar för att undvika onödig byråkrati, i synnerhet för småföretag och mikroföretag.

– I den rättsliga ramen införliva en skyldighet för registeransvariga att göra en **bedömning av hur skyddet av personuppgifter påverkas** i vissa fall, till exempel när känsliga uppgifter behandlas, eller när behandlingen i sig på annat sätt medför särskilda risker, i synnerhet när viss teknik, vissa system eller förfaranden används, däribland profilanalys och kameraövervakning.

– Ytterligare främja användningen av integritetsfrämjande teknik och den konkreta tillämpningen med hjälp av **inbyggda skyddsmekanismer**.

2.2.5. Uppmuntra självreglering och undersöka system för EU-certifiering

Kommissionen anser fortfarande att **självreglering** bland de registeransvariga kan **bidra till en bättre tillämpning av bestämmelserna om skydd av personuppgifter**. De nuvarande bestämmelser om självreglering i direktivet om skydd av personuppgifter, som ger utrymme för att upprätta uppförandekodexar[32], har hittills använts mycket sällan och anses inte tillfredsställande av privata aktörer.

Kommissionen kommer vidare att undersöka möjligheterna att inrätta ett **system för EU-certifiering (integritetsmärkning)** av integritetsskyddade processer, teknik, varor och tjänster.[33] Detta skulle inte bara ge enskilda individer vägledning i användningen av sådan teknik, varor och tjänster, utan också reglera de registeransvarigas ansvar: genom att ta fram integritetsmärkt teknik, varor eller tjänster kan den registeransvariga visa att han eller hon uppfyllt sina skyldigheter (*se 2.2.4 ovan*). Det är naturligtvis av yttersta vikt att **garantera integritetsmärkningens tillförlitlighet** och undersöka hur den passar in bland övriga rättsliga skyldigheter och internationella tekniska normer.

---

30 I fråga om integritetsfrämjande teknik, se Meddelande från kommissionen till Europaparlamentet och rådet om främjande av dataskydd genom integritetsfrämjande teknik, KOM(2007) 228. Inbyggda skyddsmekanismer för den personliga integriteten innebär att den personliga integriteten och uppgiftsskyddet beaktas i hela teknikens livscykel, från det tidiga utformningsstadiet till utbyggnad, användning och slutligt bortskaffande. Denna princip förekommer bland annat i kommissionens meddelande ”En digital agenda för Europa”, KOM(2010) 245.

31 Flera medlemsstater har genomfört den nuvarande möjligheten att låta registeransvariga utse ett uppgiftsskyddsombud för att på ett oberoende sätt se till att EU:s bestämmelser och nationella bestämmelser om uppgiftsskydd efterlevs (jfr Tysklands ”Beauftragter für den Datenschutz” och Frankrikes ”correspondant informatique et libertés [CIL]”).

32 Se artikel 27 i direktiv 95/46/EG.

33 Se i denna fråga även meddelandet om integritetsfrämjande teknik som citeras i fotnot 29.

Kommissionen kommer att

– utreda möjligheterna att **ytterligare uppmuntra självreglering**, däribland aktivt främjande av uppförandekodexar.

– undersöka om det går att inrätta **system för EU-certifiering** avseende skyddet av personlig integritet och personuppgifter.

2.3. Göra en översyn av reglerna om uppgiftsskydd inom det polisiära och straffrättsliga samarbetet

Direktivet om skydd av personuppgifter är tillämpligt på all behandling av personuppgifter i medlemsstaterna, inom såväl den offentliga som den privata sektorn. Det är emellertid inte tillämpligt på behandling av personuppgifter som ett inslag ”i en verksamhet som inte omfattas av gemenskapsrätten”, exempelvis inom det polisiära och straffrättsliga samarbetet.[34] I Lissabonfördraget har emellertid den tidigare pelarstrukturen övergivits och en ny övergripande rättslig grund införts för att skydda personuppgifter på unionens samtliga politikområden.[35] Mot bakgrund av detta, och med stöd i EU:s stadga om de grundläggande rättigheterna, understryker kommissionen i sina meddelanden om Stockholmsprogrammet och Handlingsplanen för att genomföra Stockholmsprogrammet[36] behovet av ”ett mer heltäckande system”.

Rambeslut 2008/977/RIF[37] är EU:s instrument om skydd av personuppgifter som behandlas inom ramen för det polisiära och straffrättsliga samarbetet. Rambeslutet är ett viktigt steg framåt på ett område med stora behov av gemensamma normer för uppgiftsskydd. Emellertid krävs ytterligare insatser.

Rambeslutet är enbart tillämpligt på gränsöverskridande utbyte av personuppgifter inom Europeiska unionen och inte på behandling av personuppgifter i medlemsstaterna. Denna distinktion är svår att göra i praktiken och den kan försvåra det faktiska införlivandet och tillämpningen av rambeslutet[38].

Rambeslutet medger också ett alltför omfattande undantag från principen om ändamålsbegränsning. En annan brist är frånvaron av bestämmelser om att olika uppgiftskategorier med olika grad av exakthet och tillförlitlighet bör hållas isär, att faktabaserade uppgifter bör skiljas från åsikter eller personliga bedömningar[39], samt att en

---

34 Se artikel 3.2 första strecksatsen i direktiv 95/46/EG.

35 Se artikel 16 i fördraget om Europeiska unionens funktionssätt.

36 Se KOM(2009) 262, 10.6.2009 och KOM(2010) 171, 20.4.2010.

37 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). Rambeslutet innebär endast minimal harmonisering av normerna för skydd av personuppgifter.

38 Denna distinktion förekommer inte i relevanta Europarådsinstrument som *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108.* Se även *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, ETS No.: 181 och Council of Europe Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector*, som antogs den 17 september 1987 (Samtliga texter finns tillgängliga på: www.coe.int).

39 Enligt princip 3.2 i rekommendation nr R (87) 15.

åtskillnad bör göras mellan olika kategorier av registrerade personer (brottslingar, misstänkta, offer, vittnen osv.), med särskilda garantier för uppgifter som gäller icke misstänkta.[40]

Inte heller **ersätter rambeslutet de olika rättsakter om polisiärt och straffrättsligt samarbetet som antagits inom EU**[41], och särskilt inte dem som styr funktionssätten för Europol, Eurojust, Schengens informationssystem (SIS) och tullinformationssystem (CIS)[42], vilka antingen innehåller särskilda bestämmelser om uppgiftsskydd eller vanligen hänvisar till Europarådets rättsakter om uppgiftsskydd. Vad gäller verksamhet på det polisiära och straffrättsliga området, har samtliga medlemsstater undertecknat Europarådets rekommendation nr R (87) 15, som fastställer principerna för konvention 108 för polissektorn. Rekommendationen är emellertid inte någon rättsligt bindande rättsakt.

Den rådande situationen kan direkt påverka enskilda individers möjligheter att tillvarata sina rättigheter till uppgiftsskydd på området (t.ex. att få veta vilka personuppgifter om dem som bearbetas och överförs, av vem och i vilket syfte samt om hur man tillvaratar rättigheterna, t.ex. rätten att få tillgång till dessa uppgifter).

Syftet med att införa ett samlat och konsekvent system inom EU och visavi tredjeländer är **att tillgodose behovet av en eventuell översyn av de nuvarande reglerna om skydd av personuppgifter inom det polisiära och straffrättsliga samarbetet.** Kommissionen vill betona att ett samlat system för uppgiftsskydd inte utesluter att det inom den övergripande ramen medges särskilda regler om uppgiftsskydd för polis- och rättsväsendet, med vederbörlig hänsyn till dessa områdens specifika natur enligt deklaration 21 till Lissabonfördraget. Detta visar att man exempelvis måste ta hänsyn till i vilken omfattning de enskilda fallen påverkas när det gäller det brottsförebyggande arbetet och förundersökningsarbetet samt arbetet med att upptäcka, beivra eller utdöma straff för begångna brott när en enskild person utnyttjar vissa rättigheter till uppgiftsskydd.

Kommissionen kommer i synnerhet att

- beakta **i vilken utsträckning de allmänna reglerna om skydd av personuppgifter tillämpas inom det polisiära och straffrättsliga samarbetet** samt på behandling av personuppgifter i medlemsstaterna, och om det i nödvändiga fall finns bestämmelser om harmoniserade **begränsningar** av vissa rättigheter till uppgiftsskydd för enskilda personer, t.ex. när det gäller rätten till insyn eller öppenhetsprincipen,

- undersöka behovet av att inom den nya ramen för skydd av personuppgifter införa **särskilda och harmoniserade bestämmelser**, exempelvis om uppgiftsskydd vid behandlingen av **genetiska uppgifter** i straffrättsliga syften eller om uppdelningen i olika kategorier av registrerade (vittnen, misstänkta osv.) i frågor som rör det polisiära och straffrättsliga samarbetet,

---

40 I strid med princip 2 i rekommendation nr R (87) 15 och relaterade utvärderingsrapporter.

41 Se översikten över sådana rättsakter i kommissionens meddelande Översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa – KOM(2010) 385.

42 Gemensamma övervakningsmyndigheter har inrättats genom berörda rättsakter för att säkerställa övervakning av personuppgiftsskyddet, utöver Europeiska datatillsynsmannens allmänna överbevakningsbefogenheter (EDPS) över union institutioner, organ, kontor och byråer med stöd i förordning (EG) nr 45/2001.

- inleda **överläggningar** med alla berörda parter 2011 om det bästa sättet att **se över de övervakningssystem som för närvarande används inom det polisiära och straffrättsliga samarbeett** för att säkerställa en effektiv och konsekvent övervakning av uppgiftsskyddet inom unionens samtliga institutioner, organ, kontor och byråer.

- bedöma behovet av att på lång sikt **anpassa nuvarande sektorsspecifika EU-regler om polisiärt och straffrättsligt samarbete inom ramen för specifika instrument** till den nya allmänna ramen för uppgiftsskydd.

2.4. Uppgiftsskyddets globala dimension

2.4.1. Klargöra och förenkla reglerna för internationell överföring av uppgifter

Ett av sätten att möjliggöra överföringen av personuppgifter till länder utanför EU och EES-området är att göra en s.k. **bedömning av tillfredsställande skyddsnivå**. För närvarande kan kommissionen och enskilda medlemsstater bedöma om ett tredjeland har en tillfredsställande skyddsnivå, dvs. om ett tredje land garanterar en skyddsnivå som enligt EU är tillfredsställande.

Om kommissionen anser skyddsnivån vara tillfredsställande, får personuppgifter fritt överföras från de 27 EU-medlemsstaterna och de tre EES-länderna till detta tredjeland utan att några ytterligare säkerhetsåtgärder krävs. De exakta kraven för att kommissionen ska godkänna skyddsnivån som tillfredsställande specificeras för närvarande inte tillräckligt i direktivet om skydd av personuppgifter. Inte heller innehåller rambeslutet några bestämmelser om sådana beslut av kommissionen.

I vissa medlemsstater bedöms skyddsnivån i första hand av de registeransvariga, som själva överför uppgifter till ett tredjeland, ibland i samband med den efterhandskontroll som utförs av tillsynsmyndigheten. Denna situation kan ge upphov till olika sätt att bedöma om tredjeländers eller internationella organisationers skyddsnivå är tillfredsställande och **medför en risk för att den skyddsnivå som garanteras de registrerade i ett tredjeland bedöms på olika sätt från medlemsstat till medlemsstat**. Nuvarande rättsakter innehåller heller inga ingående, harmoniserade krav på hur man bedömer om överföringar kan anses lagliga. Detta ger upphov till praktiska skillnader mellan medlemsstaterna.

Vad gäller överföringar av uppgifter till tredjeländer som inte kan garantera en tillfredsställande skyddsnivå, är kommissionens nuvarande standardklausuler för överföring av personuppgifter till registeransvariga[43] och registerförare[44] inte utformade för avtalslösa situationer och kan exempelvis inte tillämpas i samband överföringar mellan offentliga förvaltningar.

---

[43] Kommissionens beslut av den 15 juni 2010 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv 95/46/EG (EGT L 181, 4.7.2001, s. 19), kommissionens beslut av den 27 december 2001 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredje land i enlighet med direktiv 95/46/EG (EUT L 6, 10.1.2002, s. 52) och kommissionens beslut av den 27 december 2004 om ändring av beslut 2001/497/EG om standardavtalsklausuler för överföring av personuppgifter till tredje land (EUT L 385, 29.12.2004, s. 74).

[44] Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG (EUT L 39, 12.2.2010, s. 5).

När EU eller dess medlemsstater sluter internationella avtal krävs det dessutom ofta att dessa avtal inbegriper principer om uppgiftsskydd och särskilda bestämmelser. Detta kan leda till olika skrivningar med inkonsekventa bestämmelser och rättigheter, och därmed öppna för skiljaktiga tolkningar till men för den registrerade. Till följd av detta har kommissionen meddelat att den avser att arbeta med nyckelelement avseende skydd av personuppgifter i avtal mellan unionen och tredjeländer på det straffrättsliga området[45].

Andra medel som har utvecklats som en form av självreglering, såsom interna uppförandekoder för företag, även kallade ”bindande företagsregler” (*BCR*)[46], kan också vara ett användbart verktyg för att lagligen överföra personuppgifter mellan företag inom samma konsortium. Berörda parter har emellertid framhållit att denna mekanism skulle kunna utvecklas ytterligare och att genomförandet skulle kunna förenklas.

För att ovanstående frågor ska kunna behandlas **måste nuvarande system för överföringar av personuppgifter generellt förbättras**, samtidigt som det ges garantier för att personuppgifter skyddas på ett tillfredsställande sätt när de överförs till och behandlas i länder utanför EU och EES.

Kommissionen har för avsikt att undersöka hur man ska kunna

- **förbättra och strömlinjeforma nuvarande förfaranden** för internationell överföring av uppgifter samt rättsakter och bindande företagsregler för att därigenom säkerställa en **enhetligare och konsekventare EU-linje** visavi tredjeländer och internationella organisationer,

- **förtydliga kommissionen förfarande för att bedöma om skyddsnivån är tillfredsställande** och på ett bättre sätt ange **kriterierna och kraven** för bedömning av nivån på uppgiftsskyddet i ett tredjeland eller inom en internationell organisation,

- ange **nyckelelement i EU:s uppgiftsskydd** som skulle kunna användas i alla typer av internationella avtal.

2.4.2. Främja övergripande principer

Behandlingen av uppgifter är globaliserad och kräver övergripande principer om skyddet av enskilda i samband med behandling av personuppgifter.

EU:s rättsliga ram för uppgiftsskydd har ofta tjänat som **modell för tredjeländer när de inför regler om uppgiftsskydd**. Dess inflytande såväl inom som utom unionen har varit mycket betydelsefullt. **Europeiska unionen måste därför**, med utgångspunkt i gällande EU-lagar och andra EU-bestämmelser om skydd av personuppgifter, **fortsätta att driva på utvecklingen och främjandet av internationella juridiska och tekniska normer för skydd av personuppgifter**. Detta är av särskild vikt inom ramen för EU:s utvidgningspolitik.

Vad gäller internationella tekniska normer utvecklade av standardiseringsorgan, anser kommissionen att kopplingen mellan den kommande rättsliga ramen och sådana standarder är

---

45 Handlingsplanen för att genomföra Stockholmsprogrammet, *a.a.* (fotnot 36).

46 ”Bindande företagsregler” är förfaranderegler som bygger på europeiska normer för uppgiftsskydd, som multinationella organisationer utarbetar och frivilligt följer för att ge tillfredsställande garantier för överföringar eller vissa kategorier överföringar av personuppgifter mellan företag som ingår i samma konsortium eller som är bundna av dessa företagsregler. Se: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

mycket viktig för att garantera en sammanhållen och praktisk tillämpning av reglerna om uppgiftsskydd bland registeransvariga.

Kommissionen kommer att

- fortsätta att **främja utvecklingen av strikta rättsliga normer för uppgiftsskydd** i tredjeländer och på internationell nivå,

- arbeta för **principen om ömsesidigt skydd** i samband med unionens internationella insatser, särskilt i fråga om registrerade vilkas uppgifter överförs från EU till tredjeländer,

- **i detta syfte stärka sitt samarbete med tredjeländer och internationella organisationer**, såsom OECD, Europarådet, FN och andra, regionala, organisationer,

- **noggrant följa upp utvecklingen av internationella tekniska normer med hjälp av sådana standardiseringsorganisationer som** CEN och ISO, för att se till att de kompletterar rättsreglerna på ett lämpligt sätt och att de centrala uppgiftsskyddskraven verkligen tillämpas i det praktiska arbetet.

2.5. Tydligare institutionella arrangemang för en effektivare tillämpning av reglerna om uppgiftsskydd

Införlivandet och tillämpningen av principer och regler om uppgiftsskydd är centralt för att garantera respekten för individens rättigheter.

I detta sammanhang är **tillsynsmyndigheternas roll avgörande** för tillämpningen av reglerna om uppgiftsskydd. Dessa myndigheter är oberoende övervakare av grundläggande fri- och rättigheter i samband med skyddet av personuppgifter, och den enskilde är beroende av dem för att säkerställa skyddet av deras personuppgifter och lagligheten i hanteringen. Därför anser kommissionen att deras roll borde stärkas, särskilt med tanke på att EU-domstolen har utarbetat en rättspraxis enligt vilken de ska vara oberoende[47]. De borde även få nödvändiga befogenheter och resurser för att kunna utföra sina uppdrag både nationellt och när de samarbetar med varandra.

Samtidigt anser kommissionen att **tillsynsmyndigheterna bör stärka sitt samarbete sinsemellan och förbättra samordningen av sina åtgärder**, särskilt när de ställs inför frågor som är gränsöverskridande till sin natur. Detta gäller särskilt multinationella företag med sate i flera medlemsstater som bedriver verksamhet i vart och ett av dessa länder, eller när det är nödvändigt med samordnad övervakning tillsammans med Europeiska tillsynsmyndigheten[48].

I detta sammanhang **kan artikel 29-gruppen spela en viktig roll**[49]. Gruppen har, utöver sin rådgivande funktion[50], redan till uppgift att arbeta för en enhetlig tillämpning av EU:s regler

---

47 EU-domstolens dom av den 9 mars 2010, kommissionen mot Förbundsrepubliken Tyskland, mål C-518/07.

48 Detta är f.n. fallet med stora it-system, t.ex. med SIS II (jfr artikel 46 i förordning (EG) nr 1987/2006 – EUT L 318, 28.12.2006, s. 4) och med VIS (jfr artikel 43 i förordning (EG) nr 767/2008 – EUT L 218, 13.8.2008, s. 60).

49 Artikel 29-gruppen är ett rådgivande organ sammansatt av en företrädare från varje medlemsstat, tillsynsmyndigheter, Europeiska tillsynsmyndigheten (EDPS) och kommissionen (utan rösträtt), som också tillhandahåller dess sekretariat. Se även: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 Artikel 29-gruppen har till uppgift att bistå kommissionen med rådgivning om skyddsnivån inom EU och i tredjeländer samt i alla andra frågor som rör hantering av personuppgifter.

om uppgiftsskydd nationellt. Tillsynsmyndigheternas fortsatt divergerande tillämpning och tolkning av EU-reglerna, trots att uppgiftsskyddsproblemen är desamma inom hela EU, kräver att arbetsgruppens roll i samordningen av tillsynsmyndigheternas ståndpunkter förstärks på ett sådant sätt att en enhetligare tillämpning på nationell nivå och en därav följande hög nivå på uppgiftsskyddet kan garanteras.

Kommissionen kommer att undersöka

- hur **de nationella tillsynsmyndigheternas status och befogenheter kan stärkas, förtydligas och harmoniseras** inom den nya rättsliga ramen, inte minst genom att till fullo genomföra begreppet ”fullständigt oberoende”[51],

- hur man kan **förbättra samarbetet och samordningen mellan tillsynsmyndigheterna,**

- hur en mer sammanhållen tillämpning av EU:s regler om uppgiftsskydd ska kunna åstadkommas på hela den inre marknaden. Detta kan inbegripa **en stärkt roll för tillsynsmyndigheterna, bättre samordning av deras arbete genom artikel 29-gruppen (som bör tillåta mer insyn) eller en mekanism som säkerställer en sammanhållen inre marknad på Europeiska kommissionens ansvar.**

3. SAMMANFATTNING: VÄGEN FRAMÅT

Samhällets sätt att använda och sprida våra personuppgifter genomgår, precis som tekniken, ständiga förändringar. Utmaningen för lagstiftarna blir därför att stifta lagar som inte märks av tidens tand. När reformprocessen är avslutad bör EU:s regler om uppgiftsskydd också fortsättningsvis erbjuda ett starkt skydd och en god rättssäkerhet för såväl den enskilde som den offentliga förvaltningen och företagen på den inre marknaden i flera generationer. Oavsett hur komplex situationen och hur sofistikerad tekniken än är, måste det råda klarhet om vilka regler och normer som nationella myndigheter har att tillämpa och som företag och teknikutvecklare ska efterleva. Det får heller inte råda något tvivel om vilka rättigheter den enskilde har.

Kommissionens övergripande metoder för att behandla frågorna och uppnå de centrala mål som lyfts fram i detta meddelande kommer att tjäna som utgångspunkt för vidare diskussioner med övriga EU-institutioner och andra berörda parter. De kommer också i ett senare skede att utvecklas till konkreta förslag och åtgärder av både rättsligt och icke-rättsligt slag. Därför välkomnar kommissionen synpunkter på de frågor som tas upp i detta meddelande.

På grundval av detta, på en konsekvensbedömning och med beaktande av EU:s stadga om de grundläggande rättigheterna kommer kommissionen **under 2011 att föreslå lagstiftning** som syftar till en översyn av den rättsliga ramen för uppgiftsskydd, för att stärka EU:s ståndpunkt i fråga om skydd av personuppgifter på alla EU:s politikområden, också brottsbekämpning och brottsförebyggande åtgärder, med särskild hänsyn till de specifika förutsättningarna på dessa områden. Åtgärder utöver lagstiftning, såsom uppmuntran till självreglering och initiativ till en undersökning av möjligheten att införa en europeisk integritetsmärkning, kommer att genomföras parallellt.

[51] Se domstolens dom av den 9 mars 2010, kommissionen mot Förbundsrepubliken Tyskland, mål C-518/07.

I ett andra steg kommer kommissionen att **undersöka behovet av att anpassa andra rättsakter** till den nya övergripande ramen för uppgiftsskydd. Detta gäller först och främst förordning (EG) nr 45/2001, vars bestämmelser kommer att behöva anpassas till den nya övergripande rättsliga ramen. Effekterna på andra rättsakter inom denna sektor kommer också att behöva granskas ingående, men först i ett senare skede.

Kommissionen kommer även att inrätta en lämplig form av tillsyn för att kontrollera att EU-lagstiftningen på området införlivas på ett korrekt sätt. Detta kommer att ske genom att **en aktiv överträdelsepolitik bedrivs** när regler om uppgiftsskydd inte införlivas och tillämpas på ett korrekt sätt. Översynen av lagarna om uppgiftsskydd påverkar inte medlemsstaternas skyldighet att införliva och säkerställa en korrekt tillämpning av befintliga rättsakter som rör skyddet av personuppgifter[52].

Ett starkt och enhetligt uppgiftsskydd inom EU är det bästa sättet att få godkännande för och främja EU:s normer för uppgiftsskydd globalt.

[52] Detta inbegriper även rådets rambeslut 2008/977/RIF: Medlemsstater måste vidta nödvändiga åtgärder för att efterleva bestämmelserna i rambeslutet före den 27 november 2010.