Ert datum | Er referens

Datum | Vår referens
2012-03-09 | Nils Weidstam/Pär Nygårds

IT&Telekomföretagen
ALMEGA

Justitiedepartementet
Grundlagsenheten
103 33 Stockholm

Remissvar: Kommissionens förslag till dataskyddsförordning (KOM(2012)11)

IT&Telekomföretagen välkomnar EU-kommissionens ambition att stärka och harmonisera systemet för dataskydd. De stora tekniska förändringar som skett det senaste decenniet föranleder att befintlig dataskyddslagstiftning behöver moderniseras.

Utifrån Förslagets tre huvudsyften:

1. **Förbättra den inre marknaden** ur ett dataskyddsperspektiv genom att förenkla regelverket och minska administrativ börda
2. **Öka effektiviteten i det grundläggande dataskyddet och ge individen kontroll över sina uppgifter**.
3. **Förbättra samstämmigheten i regelverket för dataskydd**, inkluderande bland annat polisiärt samarbete.

samt med särskilt beaktande av syfte nummer 1:s praktiska genomförbarhet så ger IT&Telekomföretagen följande kommentarer.

Huvudsakligt verksamhetsställe

Enligt gällande EU-lagstiftning måste företag med närvaro i flera EU-länder ofta anpassa sig till flera, och ibland olika, nationella dataskyddsregler. Förslaget rekommenderar en enda lag för Europa och genom att sätta som mål att företag vilka bearbetar data i EU kommer att svara mot en enda tillsynsmyndighet på grundval av vilket land som är det huvudsakliga verksamhetsstället.

I Förslaget definieras ”**huvudsakligt verksamhetsställe**” på ett sätt som riskerar bidra till ökad förvirring snarare än att minska den.

Till exempel för att bestämma en registerförares huvudsakliga verksamhetsställe, ser förslaget till förordning till platsen för ”central administration”, en term som är odefinierad och i praktiken inte behöver ha något samband med den marknad där data i bearbetas i praktiken. Förslaget föreslår ett något mer vettigt kriterium för registerförare, beroende på var de viktigaste besluten om behandlingen tas inom EU. Då introduceras dock ett otydligt kriterium beträffande ”huvudsakligt behandlingsställe” i samband med en etablering.

Resultatet kan bli att flera dataskyddsmyndigheter hävdar jurisdiktion över organisationer, särskilt organisationer som fungerar som både registeransvariga och registerförare i flera medlemsstater.

Rekommendation från IT&Telekomföretagen: se över och förtydliga denna definition.

Registerförarens roll

Ett robust dataskyddssystem måste avgränsa ansvarsområdena för de olika parterna som deltar i bearbetningen av information och se till att parternas ansvarsbördor blir rimliga visavi deras roll i nätmiljön. I detta avseende rekommenderas det helt korrekt i Förslaget att ansvar främst placeras på registeransvariga.

Förslaget medger även utvidgade skyldigheter för registerförare. Ökade skyldigheter kan inom vissa områden vara motiverat, men då bör dessa nya ansvarsområden spegla både den komplexa avtalsmiljö där registerförare agerar samt den begränsade kontroll de ofta har över uppgifter som de behandlar. Till exempel krävs det i Förslaget att registerförare ger tillsynsmyndigheterna tillgång till uppgifter i vissa fall, uppenbarligen obeaktat eventuella konkurrerande avtalsförpliktelser.

Rekommendation från IT&Telekomföretagen*:* för att undvika eventuella motsättningar till följd av överlappande ansvar måste förändringar i ansvarsfördelningen mellan registeransvariga och registerförare noggrant övervägas i ljuset av eventuella avtalsförpliktelser som redan ålagts registerförare.

Rätten att bli bortglömd

Enligt EU-direktiv 95/46, är registeransvariga skyldiga att under vissa förhållanden radera personuppgifter på uppdrag av den registrerade. Förordningen bygger på principen att genom att individen ges en ”**rätt att bli bortglömd**” (RTBF). Enligt Förslaget skulle RTBF inte bara kräva att företag under vissa omständigheter ska radera personuppgifter efter en begäran från den registrerade, men också att data som gjorts publika ska raderas. I och med det skulle berört företag åläggas att informera alla tredje parter som bearbetat dessa data om begäran att radera kopior av hela eller länkar till dessa data. I Förslaget föreskrivs hårda sanktioner mot registeransvariga som inte uppfyller kravet.

Strukturen hos RTBF återspeglar dock inte helt strukturen av Internet. Digital data replikeras idag ofta snabbt över nätet på system och servrar över hela världen med eller utan formella teknik- eller avtalsbaserade relationer mellan olika delar av nätets ekosystem.

Till exempel har många sökmotorer och aggregatorer av innehåll som använder publikt tillgänglig information på Internet till att katalogisera och bygga stora ”cachar” av data utan uttryckligt avtal med den primära utgivaren av informationen. Dessa ”cachar” är det som gör det möjligt för individer att hitta data snabbt på internet när de gör en sökning. En följd av detta blir att kan det vara extremt svårt om inte omöjligt att ta bort alla spår. Genom att kräva att registeransvariga ska anmäla allt och samtliga tredje parter, verkar resonemanget bakom RTBF-bestämmelsen utgå ifrån att företag kan övervaka hela Internet och kontrollera informationen där. Det är en skyldighet som står i direkt strid med Internets öppna arkitektur, vilken är helt och hållet grundläggande internets utveckling och dess fortsatta bidrag till samhällsutvecklingen.

För att vara praktisk användbar får tolkningen av RTBF aldrig förpliktiga företag att göra det som är tekniskt omöjligt eller oproportionerligt.

Rekommendation från IT&Telekomföretagen: Förslaget måste begränsa RTBF till de uppgifter som lagras av och är under kontroll av den registeransvarige och är rimligt tillgängliga i den ordinarie verksamheten. RTBF bör även endast utsträcka sig till den enskilde användarens egna uppgifter (dvs. data som användaren matar in direkt) och inte de data som genererats i driften av tjänsten (till exempel felmeddelanden eller statistik över ”upptid”).

Uppgiftsportabilitet

Med den ökande användningen av online-tjänster, sociala nätverk och molntekniker för hantering av alla typer av personuppgifter, har det blivit allt viktigare för användarna att kunna ta sina data med sig när de lämnar en tjänst. Förslaget syftar till att säkerställa detta

genom att föreslå att individerna ska kunna ”portera” sina data. Men Förslaget kräver även att uppgifterna ska kunna föras tillbaka till användarna på ett sätt som möjliggör en direkt överföring till andra tjänster. Förordningen ger också kommissionen befogenhet att införa tekniska normer som styr det format som data ska returneras i.

Förslaget bör utgå ifrån faktiska tekniska förutsättningar, dvs att möjligheten att exportera data inte nödvändigtvis betyder att sådana uppgifter kompatibla med andra tjänster.

Rekommendation från IT&Telekomföretagen: utverka en lösning som tillåter användare att ”portera” de uppgifter som de ursprungligen skapat, men låt industrin besluta om format och tekniska detaljer.

Profilering

Användningen av Internet och spridningen av anslutna enheter genererar datakombinationer som aldrig tidigare förekommit. Sådana uppgifter kan ibland användas för att bygga profiler.

Profilering i sig är bara en teknisk process som hjälper till att identifiera mönster i stora mängder data, och därmed innebär att information samlas in och organiseras på ett meningsfullt sätt. Som sådan är det inget fel med profilering. I själva verket är profiler ofta använda för att tillgodose konsumenternas krav på teknik och tjänster.

Naturligtvis, som med alla affärsprocesser, kan automatiserade profiler också användas för att uppnå mindre önskvärda resultat, såsom att diskriminera personer på grund av sin hälsa. För att säkerställa att användarens data inte används för att uppnå mål som strider mot EU:s medborgares intressen är det klokt att reglera användningen av profiler för skadliga ändamål.

Rekommendation från IT&Telekomföretagen: Förslaget bör ändras för att klargöra att profiler kan fortsätta att användas för nyttiga ändamål såsom att tillhandahålla skräddarsydda Interneterfarenheter för användarna.

Dataintrång

Dataintrång är en återkommande utmaning för upprätthållandet av individens integritetsskydd. Meddelandeskyldighet vid intrång är därför viktig för att säkerställa att dataskyddsmyndigheterna och de registrerade informeras och kan vidta lämpliga åtgärder när allvarliga intrång kan vålla betydande skada.

Som Förslaget är formulerat är det dock en verklig risk att regelverket blir kontraproduktivt. Till exempel innehåller förordningen inte något tröskelvärde för när dataskyddsmyndigheter ska meddelas om en överträdelse. Istället krävs att alla registerhållare inom alla sektorer ska meddela dataskyddsmyndigheter om alla överträdelser, oavsett vikt, inom 24 timmar. Underlåtenhet föreslås leda till påföljder om upp till 2 procent av den globala omsättningen oberoende av allvaret i intrånget.,.

En konsekvens av detta förslag kan bli att dataskyddsmyndigheter snabbt bli överhopade av anmälningar, vilket försämrar deras förmåga att effektivt hantera de verkligt allvarliga brotten, ett problem som kommer att förvärras av 24-timmarstidsfristen. Detta kan leda till att registeransvariga anmäler misstänkta brott även i de fall där vidare utredning skulle ha visat att det i själva verket inte var någon överträdelse. Och medan förordningen inte omfattar en tröskel för anmälan från de registrerade (dvs. när ett brott kan orsaka ”negativa effekter¨), är tröskeln så låg att det innebär att registrerade sannolikt kommer att få konstanta meddelanden vilket kan leda till ”meddelandetrötthet¨ vilket i sin tur kan innebära att konsumenterna ignorerar meddelanden om brott. Alltför många meddelanden kan också leda till en orimlig nivå av rädsla bland europeiska Internetanvändarna vilket negativt kan påverka användningen av internet-baserade tekniker.

Rekommendation från IT&Telekomföretagen: Förslaget bör revideras till att registeransvariga ges skyldighet att endast anmäla när det finns betydande risk för allvarlig skada för den registrerade. Tidsfönstret för anmälan bör inriktas mot ”utan onödigt dröjsmål¨ snarare än inom ett 24-timmarsfönster. Stränga straff för bristande efterlevnad bör reserveras för de registeransvariga som uppsåtligen och upprepade gånger underlåter att anmäla.

Samtycke

Förslaget tillåter registeransvariga att behandla personuppgifter om den registrerade har samtyckt till behandlingen. För att säkerställa att detta samtycke är meningsfullt, innehåller Förslaget ett antal viktiga garantier, bland annat krav på att samtycke fritt ges och informeras, och att företagen tydligt mot individen särskiljer begäran om samtycke när denna är del i en bredare kommunikation.

Men utöver dessa garantier föreskriver förordningen också att samtycke måste ges på ett sätt, dvs ”explicit¨ och antingen genom ett ”uttalande¨ eller genom ”tydliga bekräftelser från den registrerade” oavsett i vilket sammanhang medgivande har givits eller data används.

Enligt förslaget kan behovet av uttalat samtycke tolkas som att det krävs att registerhållare verksamma på nätet alltid ska tvinga användare att välja ”opt-in”-godkännande vid användning av deras uppgifter. Detta tillvägagångssätt är troligtvis alltför begränsande. Det finns för närvarande ett brett sortiment av mekanismer som effektivt gör det möjligt för användare att kontrollera och samtycka till insamling och användning av information.

Rekommendation från IT&Telekomföretagen: Förslaget bör omarbetas och öppna för olika typer av godkännandemekanismer.

Ansvar

Utifrån det internationella begreppet ”ansvarighet¨ kräver Förslaget att registeransvariga och registerförare ska ”ansvara¨ för hur de hanterar data. Till exempel krävs att organisationer utser ett uppgiftsskyddsombud som ansvarar för efterlevnad. Sekretess-konsekvensanalyser (PIA) är en annan viktig del av att vara en ansvarsfull förvaltare av uppgifter och Förordningen klargör att företagen ska utföra PIA vid behandling som medför ”särskilda risker för rättigheter och friheter för de registrerade”

Dessa förslag ökar dataskyddet. IT&Telekomföretagen tror att vissa förändringar kommer att bidra till att göra dessa ansvarsskyldigheter ännu mer robusta. Till exempel avseende på PIA, anges i förordningen att registeransvariga och registerförare måste inhämta synpunkter från de registrerade när de utför en PIA och samråda med tillsynsmyndigheterna före behandlingen av uppgifterna i de fall då en PIA ”sannolikt kommer att medföra en hög grad av särskilda risker”. I detta scenario skulle de nationella myndigheterna och registrerade snabbt bli överhopade av PIA.

Rekommendation från IT&Telekomföretagen: ovanstående krav bör tas bort. Som ett minimum skulle vi välkomna att skapa klarhet i exakt när dessa regler gäller registerförare. Sådan klarhet är nödvändig, särskilt eftersom Förslaget anger att även oaktsamhet kan ge hårda straff.

Anne-Marie Fransson, förbundsdirektör,
IT&Telekomföretagen inom Almega