Prorektor Katrine Riklund/professor
Umeå universitet
090-786 50 00

UMEÅ UNIVERSITET

Utrikesdepartementet
Enheten för internationell handelspolitik
och EU:s inre marknad

ud.imremiss@gov.se
ud.registrator@regeringskansliet.se

Yttrande över Europaparlamentets och Rådets förordning om en ram för det fria flödet av icke-personuppgifter i Europeiska unionen, KOM(2017) 495

Den Samhällsvetenskapliga fakulteten vid Umeå universitet har fått möjlighet att bereda Umeå universitets yttrande över Europaparlamentets och Rådets förordning om en ram för det fria flödet av icke-personuppgifter i Europeiska unionen, KOM(2017) 495. Remissvaret baserar sig på ett underlag från Juridiska institutionen. Underlaget har utarbetats av universitetslektor Jan Leidö.

Sammanfattning

Umeå universitet konstaterar sammanfattningsvis att förslaget innehåller sådana åtgärder som är förenliga med reformens fastslagna syften; förbättra rörligheten av icke-personuppgifter, upprätthålla möjligheten för berörda myndigheters tillgång till relevanta uppgifter, samt att öka möjligheten till portering av data. I förlängningen ska detta klargöra det som i dagsläget är oklart och möjliggöra ökad konkurrens, vilket möjligtvis även leder till lägre kostnader. Baserat på dessa utgångspunkter är den valda lösningen en rimlig avvägning mellan fördelar för tjänsteleverantörer och användare å ena sidan och bördor för Medlemsstaternas myndigheter, samt att lösningen är förenlig med befintlig lagstiftning. Däremot innehåller förslaget vissa problem ur lagteknisk synvinkel, men även på en mer grundläggande nivå. Det kan inte tas för givet att förslaget verkligen kommer att åtgärda det grundläggande problemet med bristande tilltro till datasäkerhet. Gränsöverskridande avtal om datatjänster innebär också praktiskt sett större rättsliga svårigheter att utkräva ansvar och med rättsligt stöd åtgärda problem än vid inhemska avtal. Dessa underliggande problem skulle behöva utvecklas innan ett långtgående förbud mot krav på datalokalisering av icke-personuppgifter införs.

Övergripande synpunkter

Överlag innehåller förslaget åtgärder som kan uppfylla de beskrivna avsikterna. Den valda lösningen – benämnd 2a – får, som konsekvensutredningen anför, anses vara den bästa lösningen, särskilt i fråga om koherensen med befintlig lagstiftning och bördan för Medlemsstaternas myndigheter. Lösningen med självreglering i fråga om portering av data får anses vara den mest rimliga utifrån förväntade effekter i förhållande till kostnaderna. Om lösningen skulle visa sig vara otillräcklig så går det att införa rättsliga krav i framtiden. Däremot finns två aspekter som är värda att diskutera nedan, den ena mer lagteknisk, den andra mer grundläggande.

Definitioner

Som framgår av namnet på den föreslagna förordningen är objektet icke-personuppgifter. Sådana uppgifter definieras dock inte uttryckligen i den föreslagna förordningen utan måste förstås mot

Prorektor Katrine Riklund/professor
Umeå universitet
090-786 50 00

Definitioner

Som framgår av namnet på den föreslagna förordningen är objektet icke-personuppgifter. Sådana uppgifter definieras dock inte uttryckligen i den föreslagna förordningen utan måste förstås mot bakgrund av annan lagstiftning. Artikel 3.1 i den föreslagna förordningen hänvisar till artikel 4.1 i den allmänna dataskyddsförordningen (2016/679). Det finns lagstiftningstekniska fördelar med att hänvisa direkt till definitionen av personuppgifter i den allmänna dataskyddsförordningen för att motsatsvis läsa ut vad som omfattas av den föreslagna förordningen; denna lösning säkerställer att det inte uppstår konflikter i förhållande till lagstiftning avseende personuppgifter. Samtidigt innebär lösningen svårigheter för den föreslagna förordningens avnämare att förstå tillämpningsområdet. Med tanke på att reglering avseende dataskydd redan i dagsläget är komplicerad, och blir ännu mer komplicerad då den allmänna dataskyddsförordningen träder i kraft år 2018, bör fältet kanske inte göras ännu mer rättsligt komplicerat genom att inte ge ledningen i den föreslagna lagstiftningen om dess tillämpningsområde.

En lösning som undviker problemen med definitioner som kan hamna i konflikt samtidigt som den ger avnämarna viss ledning skulle vara att inkludera en icke-uttömmande uppräkning av exempel i skälen till den föreslagna förordningen för att underlätta dess förståelse. En sådan uppräkning bör dock inte formuleras på ett sätt som låser tolkningen till dessa exempel.

Krav på datalokalisering

En mer grundläggande fråga är varför krav på datalokalisering finns i dagsläget och hur detta beaktas i förslaget att i huvudsak förbjuda krav på datalokalisering. Det finns flera skäl till datalokaliseringskrav, men ett skäl som beskrivs i förslaget är bristande tilltro på datasäkerhet. Av skäl 24 i den föreslagna förordningen framgår "[o]m man stärker tilltron till säkerheten i gränsöverskridande datalagring eller annan databehandling, borde det minska benägenheten hos marknadsaktörerna och den offentliga sektorn att använda datalokalisering som ersättning för datasäkerhet." Även konsekvensanalysen visar att en bristande tilltro till datasäkerhet är en orsak till krav på datalokalisering. Lokalisering är visserligen inte en lösning på säkerhetsfrågor, men frågan är om inte första steget borde vara att upprätta tilltro till datasäkerhet innan förbud mot krav på datalokalisering införs? Förbud mot krav på datalokalisering kan möjligtvis leda till att aktörer tvingas välja leverantörer med hög säkerhetsnivå, men det är inte säkert att tilltron till datasäkerheten verkligen stärks. Med tanke på att krav i författning på datalokalisering primärt torde avse myndigheter uppstår frågan hur förbud mot datalokalisering påverkar förtroendet till sådana myndigheter om tilltron till datasäkerhet är låg? Ett första steg skulle istället kunna vara att understödja säkerhetsarbete för att höja den allmänna datasäkerhetsnivån och förhoppningsvis stärka tilliten till datasäkerhet. Med tanke på de problem med datasäkerhet som uppdagats i Sverige och andra länder nyligen borde det vara mer angeläget ur statens perspektiv än att direkt förbjuda krav på datalokalisering.

Förslaget innehåller dock en öppning för krav på datalokalisering som "är motiverat av hänsyn till allmän säkerhet." Som framgår av skäl 12 i förslaget ska detta tolkas utifrån den generella förståelsen av begreppet, uttryckt särskilt i artikel 52 i Funktionsfördraget och med beaktande av proportionalitetsprincipen. Således måste undantaget tolkas snävt. Detta är fördelaktigt utifrån förslagets syfte – att öka rörligheten av icke-personuppgifter – men utifrån den bristande tilltron till datasäkerhet kan det uppfattas som problematiskt att drastiskt begränsa möjligheterna till datalokalisering. Det kan visserligen finnas en risk att nationella lagstiftare inför krav på datalokalisering som en reaktion på osäkerhet kring datasäkerhet, men då är problemet återigen tilltron till datasäkerhet, inte nödvändigtvis en vilja att gynna nationella tjänsteleverantörer.

Prorektor Katrine Riklund/professor
Umeå universitet
090-786 50 00

UMEÅ UNIVERSITET

Förslaget tar sikte på tillgång till uppgifter för behöriga myndigheter, eftersom detta beskrivs som en farhåga och orsak till kraven på datalokalisering. Denna bestämmelse är i sammanhanget därför nödvändig. Men tillgång till uppgifter torde inte vara den enda orsaken till krav på datalokalisering i dagsläget. Från ett rättsligt perspektiv är det rent praktiskt mycket enklare att utkräva ansvar, såväl civilrättsligt som straffrättsligt, gentemot aktörer lokaliserade i den egna medlemsstaten och när data också befinner sig på servrar i den egna medlemsstaten. Det som är speciellt för avtal rörande datatjänster är behovet av att snabbt, med rättsliga verktyg som stöd, kunna åtgärda problem och risker. Även möjligheterna till rättsligt ansvarsutkrävande i efterhand kan försvåras när avtalet avser digitala tjänster.

Ett enskilt företag som avser ingå avtal om t.ex. en datalagringstjänst måste väga samman datasäkerhetsrisker och rättsliga risker och möjligheter att kunna utkräva rättsligt ansvar. I vissa situationer kan det då vara rationellt med krav på datalokalisering. Den föreslagna förordningen tar endast sikte på krav på datalokalisering i nationell lag eller annan författning, enskilda aktörer kan fortfarande välja såväl inhemska som utländska tjänsteleverantörer. Den svenska IT-debatten har under senare tid fokuserat på att varken myndigheterna själva eller regeringen tycks ha fullständig insikt och överblick över användning av IT-tjänster. Med beaktande av detta är det förståeligt om stater vill kunna kontrollera detta genom krav på datalokalisering. Även om det möjligtvis skulle leda till högre kostnader är det utifrån statens perspektiv möjligt att argumentera för att detta vägs upp av lägre rättsliga risker. Vissa av dessa situationer skulle antagligen omfattas av undantaget om "allmän säkerhet", men troligtvis inte alla. För att minska den rättsliga osäkerheten inför gränsöverskridande avtal finns det anledning att se över möjligheten att snabbt och enkelt kunna utkräva ansvar och med rättsligt stöd åtgärda problem. De befintliga lösningarna för att rättsligt utkräva ansvar kan för avtalstypen inte anses vara särdeles snabba.

Förslaget med förbud mot datalokalisering är lovvärt för att förbättra den europeiska marknaden på området, men innan ett sådant förbud införs bör de underliggande problemen med bristande tillit till datasäkerhet ses över, liksom de praktiska rättsliga svårigheterna med att utkräva ansvar som i dagsläget kan göra det rationellt att välja en inhemsk leverantör.

Beslut i ärendet har fattats av prorektor Katrine Riklund efter föredragning av fakultetssamordnare Åsa P Isaksson.

Umeå som ovan

Katrine Riklund
Prorektor