IT SÄKERHETSBOLAGET

Skrivelse om molntjänster
2021-10-19
Liv Zettergren, IT-jurist

Om molntjänsters juridiska status

Molntjänster är beteckningen på allehanda IT-tjänster som finns tillgängliga online eller från någon annan plats än de egna lokalerna. Det kan vara fråga om applikationer, plattformar och infrastruktur och kan exempelvis utgöras av mjukvaruprogram som vi kommer åt via en uppkoppling.

Den aktuella Schrems-debatten har i mångt och mycket kretsat kring begreppet ”tredjelandsöverföringar”, något som aktualiseras i många molntjänster. En tredjelandsöverföring blir till när personuppgifter tillgängliggörs utanför EU, till exempel på grund av att lagring sker på plats utanför unionen, men även då en supportfunktion är fysiskt placerad i en annan region. Sådana överföringar *kan* vara tillåtna om det finns stöd i GDPR:s 5:e kapitel.

Exempel på lagstöd för tredjelandsöverföringar kan vara att EU-kommissionen beslutat att ett lands lag når upp i ”adekvat skyddsnivå” (såsom Israel, Schweiz eller Japan). Andra lagstöd kan vara att den personuppgiftsansvarige vidtagit *lämpliga skyddsåtgärder* inför överföringen. Sådana åtgärder kan bestå av att parterna ingått bindande företagsbestämmelser (BCR) eller tillämpar EU:s standardavtalsklausuler (SCC). Lämpliga skyddsåtgärder måste dock alltid kompletteras med lagstadgade rättigheter för registrerade och tillgängliga effektiva rättsmedel (art. 46.1 GDPR). Om det, liksom vanligtvis, är fråga är om överföring till ett personuppgiftsbiträde måste också den personuppgiftsansvariga utreda om biträdet kan ge tillräckliga garantier för en säker behandling (28.1 GDPR).

I Schrems-domen ogiltigförklarades lagstödet för den överföring som Facebook grundade sina tredjelandsöverföringar på (”Privacy Shield” som var en överföringsmekanism som gällde mellan EU och USA vid tiden för överföringen). Shrems-målet handlade dock inte primärt om just tredjelandsöverföringar som sådana, utan om en annan mycket viktig fråga - EU-medborgares rättigheter. Domens kontenta var att de *rättigheter* som GDPR tillerkänner oss EU-medborgare inte kan tillhandahållas av USA.

När ett företag som har åtkomst till (person-)data omfattas av amerikansk rätt så finns en risk för att amerikanska myndigheter (såsom säkerhetspolisen) kan tvinga det amerikanskägda företaget att lämna ut (person-)uppgifterna till myndigheten. Bland regelverken kan nämnas FISA 702, Executive order och Cloud Act.

Enligt GDPR har vi bland annat rätt till information om hur våra personuppgifter behandlas. En amerikansk utlämningsorder är dock ofta sekretessbelagd, varför regelverken går stick i stäv. Det utlämnande företaget får inte tillämpa transparens i frågan enligt amerikansk rätt, vilket omöjliggör för samma företag att efterleva GDPR (och dess principer och rättighetskatalog).

Schremsdomen handlade alltså inte om molntjänster som sådana, utan om olika regelverks förhållande till varandra. Begreppet molntjänst har dock blivit så laddat idag att såväl företag som myndigheter väljer att i stället nyttja andra, ofta mindre säkra lösningar.

IT-Säkerhetsbolaget AB
Storgatan 73
852 33 SUNDSVALL

Telefon:
060 - 55 62 60

E-mail:
info@itsakerhetsbolaget.se

Webb:
www.itsakerhetsbolaget.se

Orgnr: 556915-8990

Utredning av molntjänst

Vad som är viktigt att ur Schrems-perspektiv beakta för en laglig användning av en molntjänst är:

- **Görs det tredjelandsöverföringar?**

Om nej så finns ingen problematik enligt Schrems-domen, utan den personuppgiftsansvarige ska vidta tekniska och organisatoriska säkerhetsåtgärder för att skydda uppgifterna, exempelvis inom ramen för ett personuppgiftsbiträdesavtal.

- **Vilket lands lag lyder företaget (som överföringen görs till) under?**

Ett amerikanskt företag lyder exempelvis under amerikansk lag om det har sitt huvudkvarter i USA. Här behövs mottagarlandets inhemska rätt beaktas.

- **Finns det lagstöd för eventuella tredjelandsöverföringar till landet dit överföringen görs?**

Om det finns lagstöd för överföringen ska en utredning vidtas av huruvida det finns lagstadgade rättigheter och effektiva rättsmedel för de registrerade i det mottagande landet.

Ovannämnda frågeställningar ska inte beaktas som uttömmande för att behandlingen ska vara laglig ur ett GDPR-perspektiv. Däremot är de avgörande för frågan huruvida en molntjänst är laglig eller ej.

Något om sekretess

Det finns också frågeställningar som med anledning av den svenska offentlighets- och sekretesslagstiftningen måste beaktas inför användningen av en molntjänst:

- **Behandlas sekretessbelagda uppgifter?**

Det faktum att myndigheter behandlar sekretessbelagd information i molntjänster har föranlett diskussioner om en sådan ordning är förenlig med *offentlighets- och sekretesslagen (2009:400)*. Leverantörernas tystnadsplikt har tidigare i bästa fall reglerats genom civilrättsliga avtal och har på så vis varit begränsad, eftersom eventuella överträdelser inte har omfattats av straffsanktioner. I en ny *lag om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (2020:914)* har det underlättats för myndigheter att utkontraktera tillhandahållandet av it-tjänster till privata aktörer. Lagen föreskriver tystnadsplikt för den som på grund av anställning eller på något annat sätt deltar i eller har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet *tekniskt bearbeta eller tekniskt lagra uppgifter*.

I propositionen exemplifieras detta såsom *åtgärder i samband med att införa, förvalta, utveckla och avveckla en tjänst, exempelvis förändringar av funktionen för en tjänst, införande av tilläggstjänster och supporttjänster*. Vidare nämns åtgärder med *säkerhetskopiering, uppgraderingar och uppdateringar samt export av information vid avveckling av en tjänst*. Tystnadsplikten är avsedd att motsvara den sekretess som gäller för myndigheternas egen personal i motsvarande fall och kan komma att ersättas med eller kompletteras med en sekretessbrytande bestämmelse i OSL.