

Rättsläget för amerikanska molntjänster

Uppdaterat: 2023-10-31

- Konsekvensen av GDPR kapitel V om tredjelandsöverföringar är att bl.a. amerikanska molntjänster inte lever upp till lagkraven enligt GDPR.
- Exempel på amerikanska molntjänster är Google, Facebook, Instagram, LinkedIn, Microsoft 365, AWS etc.
- Fram till den 16 juli 2022 var dock rättsläget i detta avseende oklart, eftersom den s.k. **Privacy Shield** fanns, ett juridiskt ramverk för hur överföring av personuppgifter för kommersiella syften fick gå till mellan EU och USA. Det var den numera världsberömda **Schrems II-domen** från juni 2020 som satte stopp för Privacy Shield. Fr.o.m. då var det tydligt olagligt i EU enligt GDPR att behandla personuppgifter i amerikanska molntjänster. Detta förbud gällde alla sorters personuppgifter och inte bara känsliga personuppgifter, eftersom GDPR gäller för alla sorters personuppgifter.
- Den 10 juli 2023 kom det länge omtalade s.k. **adekvansbeslutet** mellan EU och USA. Innebörden av detta är att det nu finns ett av EU godtagat ramverk för självcertifiering som amerikanska molntjänstleverantörer kan använda sig av för att uppnå de nu förenklade förutsättningarna för GDPR-efterlevnad. Amerikanska företag som har certifierat sig själva publiceras på EU:s officiella lista:
<https://www.dataprivacyframework.gov/s/participant-search>. Adekvansbeslutet står dock på juridiskt instabil grund. Dels har både EU-kommissionen och EU-domstolen invändningar som kommer att prövas inom 12 månader, dels har österrikaren Max Schrems aviserat att det kommer att bli en Schrems III-dom, dels har fransmannen Philippe Latombe dragit igång en process för att överpröva lagligheten i

adekvansbeslutet som inriktar sig på andra juridiska brister än de som Schrems fokuserar på.

- Svenska Esam anser att det inte är tillräckligt att ett företag finns med på EU:s officiella lista för att det ska vara grönt ljus enligt GDPR, utan att lagligheten beror på vad för personuppgifter som behandlas och hur behandlingen går till. Esam har nu i oktober 2023 publicerat en metodik för att kunna avgöra detta. Sammantaget är det enligt deras bedömning idag många fler slags personuppgiftsbehandlings i amerikanska molntjänstlösningar som passerar nålsögat än tidigare.
- Rättsläget är nu alltså återigen oklart, eftersom adekvansbeslutet vilar på instabil grund och avgörande frågor i sammanhanget kommer att börja klarna först om ett år. Mycket talar också för att när rättsläget har klarnat efter ytterligare några år när också de pågående Schrems och Latombe-målen har avgjorts, så kommer det att visa sig att tillbaka i den situation som rådde efter Schrems II, eller att det t.o.m. blivit ännu tydligare att behandling av personuppgifter inte är möjligt i amerikanska molntjänster för organisationer verksamma i EU. Skälet till detta är att rättsvårdande instanser i EU har att förhålla sig till gällande rättsliga och tekniska förutsättningar, och de rättsliga och tekniska förutsättningarna har i princip inte ändrats alls utöver adekvansbeslutet (som är en rent politisk produkt). Den faktiska förändring i rättsläget som har ägt rum, är att USA:s president i en s.k. presidentorder (**US Executive Order 14086**) har infört ett rekvisit om proportionalitet – men vad som är proportionerligt enligt amerikanska myndigheter vet vi redan idag att det skiljer sig från vad som anses vara proportionellt enligt EU:s standarder.

Den juridiska problematiken – krockande jurisdiktioner

- Grundproblematiken är tvåsidig, och har att göra med dels den legala miljön i USA, dels med hur dessa tjänster idag är tekniskt utformade.

- Vad gäller **den legala miljön i USA** så har amerikanska myndigheter genom de amerikanska lagarna **Cloud Act** och **FISA 702** rätt att när som helst få tillgång till personuppgifter som behandlas av företag som har amerikanska ägare. **Detta problem gäller oavsett de tekniska förutsättningarna i de amerikanska molntjänsterna.** När GDPR trädde i kraft den 25 maj 2018 blev amerikanska molntjänster olagliga. GDPR:s innehåll hade då varit internationellt känt i alla detaljer i 2 år. När **Cloud Act** trädde i kraft i februari 2018, och den tillfälliga lagen **FISA 702** beslutades att förlängas med 6 år också i februari 2018, var det alltså fullt medvetet att de skulle krocka med GDPR – det hade förts ingående diskussioner mellan EU och USA om detta i förväg (enligt Daniel Melin på Skatteverket, som är en svensk GDPR-guru). **Cloud Act** handlar om rättsvårdande myndigheter typ FBI. **FISA 702** är dock ännu viktigare ur GDPR-synpunkt (och Schrems II handlar om hur långtgående denna lag sträcker sig) – NSA lutar sig på denna lag, de motsvarar FRA i Sverige och det innebär att det finns ett antal punkter i världen där NSA tappar av all datatrafik som passerar. **Kryptering är inte i sig en tillräcklig lösning för att skydda personuppgifter långsiktigt så som GDPR tar sikte, och det finns idag inga tekniska eller kontraktuella åtgärder som man kan vidta för att skydda sig mot FISA 702 när det gäller amerikanska molntjänster, enligt Daniel Melin** (här måste alltså någon form av lagändring till!). FISA är från 2008 och har sina rötter i 11 september-händelserna i USA, tillägg 702 är en tillfällig lag som först beslutades 2008 och därefter har förlängts flera gånger. Det har nu gått tre år sedan GDPR trädde i kraft, och det syns inga tecken på att USA håller på att ändra **Cloud Act** eller **FISA 702**, trots att **Schrems II** har medfört att alla organisationer i EU (som håller koll på GDPR och de problem med amerikanska molntjänster som har debatterats i tre års tid) nu har fått kalla fötter inför amerikanska molntjänster, vilket ju helt uppenbart utgör seriösa hot mot de amerikanska molnföretagens marknadsandelar i EU.
- Vad gäller **de tekniska problemen** med de amerikanska molntjänsterna så har det att göra med leveransmodellerna. Infrastrukturen har (liksom företagen) sin bas i USA, och vid stor belastning på en marknad i EU används servrar i USA för databehandlingen. Det är idag alltså bara tekniska åtgärder som kan åtgärda de problem som Schrems II lyfter – avtal räcker inte. Amazon AWS har t.ex. idag en klausul i sina molnavtal om att i händelse av att amerikanska staten vill bereda sig tillgång till personuppgifter som Amazon förfogar över, så kommer Amazon att bestrida detta anspråk. I realiteten kommer det bestridandet då att hamna i amerikansk domstol (eftersom det är ett amerikanskt företag), och det är då sannolikt att den amerikanska domstolen kommer att döma i enlighet med amerikansk lagstiftning. Det man kan och måste göra tekniskt är dels att **kryptera** de personuppgifter som behandlas i amerikanska molntjänster, och detta måste göras på ett sådant sätt att den personuppgiftsansvarige har egna krypteringsnycklar hos leverantören, alternativt om leverantören är i EU och har egna nycklar som amerikanska staten inte kan få tillgång till så räcker det också. Dels att ändra formatet, d.v.s. **pseudonymisera**, eller en kombination av kryptering och formatändring. Vad specifikt gäller Amazon AWS så finns det ett numera välkänt utlåtande av franska **Conseil d'Etat-utlåtandet från mars 2021**. Den bild som ges av

detta utlåtande är att Amazon AWS är en amerikansk molntjänst som är säker att använda ur GDPR-synpunkt därför att Amazon ger sina kunder kontroll över krypteringsnycklarna. Daniel Melin på Skatteverket har dock framhållit att detta franska utlåtande inte är någon dom, och juridiskt sett har mycket begränsad räckvidd utanför detta mycket specifika fall där och då i Frankrike.^[1]

- **Givet det nu sagda landar problemet med amerikanska molntjänster i att användandet av dem förutsätter att datat krypteras för amerikanska staten, och än så länge tillhandahåller inte någon av de amerikanska molntjänsterna en sådan kryptering.** De krypteringslösningar som idag erbjuds av t.ex. Microsoft innebär bara att man knyts ännu hårdare fast till Microsoft samtidigt som Microsoft alltså behandlar datat olagligt enligt GDPR och det är vi som personuppgiftsansvariga som ansvarar inför IMY. Det är också viktigt att förstå detta, eftersom Microsoft påstår sig vara GDPR-compliant men inte är det, och eftersom Microsoft är väl insatta i allt det ovannämnda och diskuterar om allt detta i termer att nu har Microsoft löst alla problem som tidigare framkommit genom Schrems II (detta är Huddinge kommuns erfarenhet av förhandlingarna under våren 2021). Överför man personuppgifter till USA via en amerikansk molntjänst, så måste man alltså i enlighet med **Schrems II** ha *andra* säkerhetsåtgärder på plats än de som idag ingår i de stora amerikanska molntjänsternas tekniska lösningar. Än så länge finns det inga tekniska krypteringslösningar på plats genom andra aktörer som är kompatibla med de amerikanska molntjänsterna (men detta behöver nyhetsbevakas!).

Vilka förtydliganden och förändringar i rättsläget har skett sedan 2020?

- Schrems II-domen förtydligade alltså rättsläget kring amerikanska molntjänster, och att personuppgiftsbehandling i sådana är olaglig enligt GDPR (d.v.s. rättsläget ändrades inte, och det blev inte otydligare i och med Schrems II).

- Europaparlamentet har, givet detta rättsläge som det är uppenbart sedan GDPR trädde i kraft 2018 att det är svårhanterligt för alla organisationer i hela EU, antagit en **resolution den 20 maj 2021** med anledning av Schrems II (12 sidor) och i juli 2021 publicerat studien **Exchanges of Personal Data after the Schrems II Judgment** (122 sidor).
- EU:s centralorgan för dataskydd EDPB har i juni 2021 publicerat både riktlinjen **EDPB 01/2020** (48 sidor) och **EU Cloud Code of Conduct** (84 sidor). Den sistnämnda, som här förkortas **ECCC**, är den första sådana uppförandekoden som avses i GDPR artikel 40 och 41 och tog 9 års politiskt och juridiskt arbete att ta fram. Den hör till den sorts extra säkerhetsåtgärder som är avsedda att lösa problemen med de amerikanska molntjänsterna i EU. Men tyvärr löser inte **ECCC** i sin nuvarande form de befintliga problemen fullt ut (återigen: det krävs tekniska förändringar för att komma tillrätta med problematiken). Full efterlevnad av **ECCC utgör alltså *inte* idag tillräckliga säkerhetsåtgärder för att kunna använda amerikanska molntjänster**. Att certifiera sig enligt **ECCC** är ett sätt att åta sig att följa denna uppförandekod, men det är inte samma sak som att man är godkänd enligt GDPR. Däremot är sådan certifiering ett sätt att visa att man har dokumentation på att man följer de rekommendationer som finns från högsta ort för hur man ska leva upp till GDPR. Av ECCC och EDPB 01/2020 följer sammantaget att personuppgifter ska vara både pseudonymiserade och "state of the art"-krypterade för att tillåtas överföras till företag som lyder under amerikansk lagstiftning.
- Inför **adekvansbeslutet i juli 2023** skedde en liten, men för adekvansbeslutets realiserande uppenbarligen avgörande justering i det amerikanska rättsläget. Nämligen att den nya amerikanska presidentordern **US Executive Order 14086**, som är ett avsiktligt steg att närma sig EU:s krav för skydd av personuppgifter som överförs till USA från EU, ska innehålla ordet "proportionerligt". Vad som är "proportionerligt" finns det dock ingen överenskommelse om mellan EU och USA, och vi vet att det i enlighet med FISA 702 anses proportionerligt med massövervakning enligt amerikansk rätt medan EU betraktar massövervakning som oproportionerligt. Dessa skillnader i tolkning måste alltså prövas i EU-domstolen innan vi vet säkert om EU:s nuvarande eller USA:s nuvarande tolkning står sig rättsligt i EU. Detta är bl.a. vad Max Schrems är inriktad på att driva.
- Förutom GDPR förbjuder även den nya svenska **lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter** in sin § 4 lagring i amerikanska molntjänster, givet **Cloud Act** och **FISA 702**. Detta ändras nu också av adekvansbeslutet, men kan ändras tillbaka om adekvansbeslutet inte står sig.

[1] <https://www.linkedin.com/pulse/den-franska-domen-som-%C3%A4r-ett-beslut-daniel-melin/?originalSubdomain=se>

Revisions #2

Skapad 3 juni 2025 09:17:31 av Jakob Söderbaum

Uppdaterad 3 juni 2025 14:45:45 av Jakob Söderbaum