

Författare:

Martin Whitworth

juli 2019

Bli inte skrämdd av CLOUD Act

CLOUD Act

I mars 2018 beslutade USA om en lagstiftning som syftar till att reglera hur myndigheter, domstolar, polis och åklagare (law enforcement) ska kunna begära ut data som lagras utanför de nationella gränserna: The Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

Syftet med CLOUD Act är att upprätta bilaterala avtal som ger amerikanska myndigheter åtkomst till data som är relevanta i ett givet rättsfall och som lagras utomlands, i utbyte mot att låta utländska regeringar få åtkomst till data som lagras i USA.

Om ett sådant bilateralt avtal inte finns med ett land eller en region, och begäran av data strider mot lokala lagar om integritetsskydd, har leverantörer av respektive molntjänst möjlighet att försöka ogiltigförklara begäran från de amerikanska myndigheter som begärt uppgiften.

Den här rapporten syftar till att klargöra hur CLOUD Act kommer, och inte kommer, att påverka användningen av molntjänster och vilken påverkan den får på molntjänstleverantörer.

Fakta (och myter) om CLOUD Act

Det finns mer än tillräckligt med osäkerhet, förvirring och missförstånd när det gäller CLOUD Act. Det har lett till otaliga påståenden och myter, vilket gör att fakta behöver läggas fast och göras tydliga.

CLOUD Act ger inte brottsbekämpande organ i USA obegränsad åtkomst till personuppgifter

Polis och åklagare (i CLOUD Act benämnda Law Enforcement) i USA kan endast begära innehåll från tjänstleverantörer om den som data berör (den fysiska eller juridiska person som innehar rättigheterna till datat) har samtyckt eller om en fullmakt har utfärdats av en amerikansk domstol i enlighet med CLOUD Act eller i enlighet med ett överenskommet bilateralt avtal. Ett bilateralt avtal kan vara i form av ett fördrag mellan länder, men i hittills förekommande fall har det skett i form av ett så kallat "exekutivt avtal", där presidentämbetet i USA direkt gör avtalet med respektive region eller enskilt land.

Molntjänstleverantörer kan hjälpa till att skydda kunders innehåll

CLOUD Act innehåller inga bestämmelser att dela krypteringsnycklar och molntjänstleverantörer har möjligheter att erbjuda en mängd olika tjänster för att förbättra säkerheten och skyddet av kunddata.

Det finns mer än tillräckligt med, osäkerhet, förvirring och missförstånd när det gäller CLOUD Act.

CLOUD Act bortser inte från, ersätter inte och förändrar inte ett annat lands lokala lagar.

Åtkomst till data utanför landets gränser kräver bilateralt avtal

CLOUD Act skapar en ny process för amerikanska myndigheters möjlighet att få åtkomst till data lagrad utanför landets gränser. Den skapar också ett nytt regelverk för USA för hur bilaterala avtal med andra regioner eller enskilda länder ska hanteras och hur en begäran om data från myndigheter i USA ska hanteras. Om det inte finns något bilateralt avtal måste en begäran om data genomgå den sedvanliga processen för ömsesidigt rättsligt bistånd (Mutual Legal Assistance Treaty – MLAT ([läs mer på https://www.mlat.info/](https://www.mlat.info/)), vilket är en existerande process och inte innebär en förändring från tidigare.

CLOUD Act ger ömsesidig åtkomst

CLOUD Act syftar till att ge ömsesidig åtkomst till data mellan USA och motparten i det bilaterala avtalet, och då alltid genom en överenskommen och godkänd rättslig process.

CLOUD Act har inte företräde framför befintliga lagar

CLOUD Act bortser inte från, ersätter inte och förändrar inte ett annat lands lokala lagar. Faktum är att CLOUD Act erkänner tjänsteleverantörers rätt att bestrida en begäran som strider mot ett annat lands lagstiftning eller nationella intressen.

CLOUD Act och molntjänstleverantörer

I tillägg till ovanstående myter, finns det flera påståenden som är särskilt riktade till molntjänstmarknaden.

CLOUD Act är inte inriktad på molntjänstleverantörer

Trots att globala molntjänstleverantörer lagrar stora mängder data som amerikanska brottsbekämpande organ skulle kunna få åtkomst till enligt CLOUD Act, är molntjänstleverantörer inte de enda möjliga eller sannolika mottagarna av en fullmakt. Alla organisationer som arbetar från USA och lagrar data utanför USA omfattas av denna lagstiftning i samma utsträckning som molntjänstleverantörer.

CLOUD Act gäller inte endast molntjänstleverantörer

CLOUD Act gäller alla organisationer som har sitt säte i eller anses arbeta från USA och som tillhandahåller elektroniska kommunikationstjänster eller tjänster för åtkomst till servrar och data på distans (remote access), till användare och kunder (inklusive e-post och molntjänstleverantörer), oavsett om tjänsterna tillhandahålls i USA eller ett annat land.

Det finns inga bestämmelser om dekryptering

Det finns inga bestämmelser i CLOUD Act som ger skyldighet till dekryptering av data som molntjänstleverantörer lagrat på uppdrag av sina användare eller kunder. Lagen skapar inte ett enkelt sätt för avkodning som polis och åklagare kan använda sig av för att dekryptera data som kontrolleras av slutanvändaren. Det är viktigt att förstå att även om data som krypterats av en molntjänstleverantör kan lämnas ut genom domstolsbeslut, kan data som krypterats av kunden inte dekrypteras av molntjänstleverantören.

Risken för konflikt mellan CLOUD Act och GDPR hänger på om USA och EU kan förhandla fram ett avtal som tillfredsställer båda parter.

Mycket av osäkerheten skapas av lokala tjänsteleverantörer

CLOUD Act är ett nytt regelverk, men den ger inga förslag om att en tjänsteleverantör inom eller utom landet är att föredra. Företag och organisationer, måste förstå vilken kapacitet och ställning varje potentiell molntjänsteleverantör har, i vilken mån de exempelvis kan erbjuda kundstyrd kryptering, konfigurerbara regionala datalager och hur de tillhandahåller tjänster som bäst passar verksamheten osv.

Vad innebär det för molntjänsteleverantörer?

Molntjänsteleverantörer kan vara en utmärkt resurs för att hjälpa företag och organisationer att navigera genom komplexiteten i CLOUD Act, särskilt när det gäller hur den påverkar verksamheten. Molntjänsteleverantörerna behöver vara mycket tydliga vad gäller de tjänster de erbjuder och vilket stöd tjänsterna har för skydd av kunddata, till exempel datasegmentering, kryptering och hantering av krypteringsnycklar. Slutligen måste molntjänsteleverantörer kunna samarbeta med sina kunder för att tydligt definiera ansvar för och hantering av en potentiell begäran från amerikanska myndigheter.

Måste regionala tjänsteleverantörer följa CLOUD Act?

Trots att regionala (i meningen "inte baserade i USA") tjänsteleverantörer inte omfattas specifikt av CLOUD Act, är det sannolikt att de omfattas av en amerikansk myndighets begäran om data i det fall att de nödvändiga avtalen förhandlats fram. Dessutom förväntas de fortfarande svara på begäran som görs via Mutual Legal Assistance Treaty (MLAT) och en sk "letters of rogatory" (<https://legal-dictionary.thefreedictionary.com/letters+rogatory>). När man överväger en molntjänsteleverantörs tjänster ska man göra kontroller och få en tydlig förståelse för vilka möjligheter och förmågor molntjänsteleverantören har– och därefter fatta ett beslut. Viktigast av allt är att inte fatta förhastade beslut och inte falla offer för tvivel och osäkerhet.

CLOUD Act och GDPR

Minimal konflikt

Det finns en mängd ogrundade påståenden om konflikter mellan CLOUD Act och EU:s GDPR. Det finns i själva verket endast ett område med potentiella problem och det gäller dataöverföring till länder utanför EU och framför allt, en potentiell konflikt mellan avsnitt 2713 i CLOUD Act (<https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>) och artikel 48 i GDPR (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>).

Lösningar?

För att lösa detta behöver man bedöma två olika scenarier:

- **Om det finns ett bilateralt avtal på plats** måste alla detaljer om vad som är eller inte är tillåtet utarbetas av de två parterna (USA och dess motpart – EU eller ett enskilt land) och låta domstol besluta om avtalet eller GDPR har företräde.

- **Om det inte finns något bilateralt avtal på plats** beror all överlämning av uppgifter på hur tjänsteleverantören reagerar på den fullmakt som amerikanska myndigheter har utfärdat. Tjänsteleverantören har rätt att försöka ogiltigförklara fullmakten baserat på den konflikt med lokala lagar (i detta fallet GDPR) som finns.

Risken för konflikt mellan CLOUD Act och GDPR beror på om USA och EU kan förhandla fram ett avtal som tillfredsställer båda parter. För tydlighets skull är det dock endast företag som förvaltar data/information relaterat till ett allvarligt brott som skulle påverkas. EU-kommissionen är också i färd med att skapa EU:s motsvarighet till CLOUD Act – kallad förordning om tillgång till e-bevisning. Med både CLOUD Act och förordningen om tillgång till e-bevisning på plats skulle det finnas en grund till ett bilateralt avtal mellan USA och EU som eliminerar eventuella konflikter med GDPR eller annan lagstiftning knutet till ett visst land.

Möjligheten att ogiltigförklara är mycket begränsad

Observera även att möjligheten för en molntjänstleverantör att försöka ogiltigförklara en fullmakt om åtkomst till en kunds information som är baserad på CLOUD Act endast gäller om:

- Den kunden är en fysisk person som inte är en amerikansk medborgare och inte är bosatt i USA, eller om
- Den kunden är en juridisk person som inte har sitt säte i, eller utgår från USA. Utlämnandet som krävs skulle skapa en reell risk att leverantören skulle strida mot lagarna i det landet.

Därför finns det fortfarande en möjlig motsättning om en amerikansk medborgare som är bosatt i EU är föremål för en fullmakt inom ramen för CLOUD Act.

Vad gäller för Brexit?

USA och Storbritannien förhandlar redan om ett avtal som ska möjliggöra ett skydd för samhälle, för nationell säkerhet och för brottsbekämpande myndigheter. För tillfället finns inga detaljer om avtalet, men det kommer sannolikt att återspegla tidigare avtal om informationsutbyte för nationell säkerhet och brottsbekämpning. Eftersom Storbritannien kommer att lämna EU under 2019 är inte GDPR direkt aktuell, men Storbritannien har redan antagit den brittiska lagen om skydd av personuppgifter 2018 (vilken implementerar GDPR med vissa givna undantag, tillägg och särskilda bestämmelser för Storbritannien). Dessa kommer att hanteras av avtalet.

Sammanfattning

CLOUD Act är på plats och har ännu inte prövats i domstol, men verksamheten i företag och organisationer måste fortsätta. Det viktiga är att behålla lugnet – några grundläggande principer är viktiga att komma ihåg:

- Endast data som är relevanta för att skydda den offentliga säkerheten och bekämpa allvarliga brott, terrorism inkluderat, omfattas av CLOUD Act.

CLOUD Act är på plats och har ännu inte prövats i domstol, men verksamheten i företag och organisationer måste fortsätta.

- Dina molntjänstleverantörer är dina partners, så prata med dem och undersök vad de kan göra och hur de ställer sig till amerikanska myndigheters processer och regelverk gällande CLOUD Act.
- Kryptering är din vän. Förutom att kryptering minskar oron för insiders hos tjänsteleverantören eller hackerattacker från utomstående blir dessa data värdelösa för en utomstående i den händelse att tjänsteleverantören måste lämna över data som en del av en begäran från en amerikansk eller annan statlig myndighet, utan ditt företags hjälp.
- Se till att du har tillräcklig information om CLOUD Act och annan lokal lagstiftning som kan påverka din verksamhet.
- Enligt CLOUD Act görs en begäran om tillgång och överlämning av data antingen genom en fullmakt utfärdad av en amerikansk domstol (som kan ifrågasättas om den står i konflikt med lokala lagar) eller via ett bilateralt avtal mellan USA och en region eller enskilt land.
- Vid val av tjänsteleverantör är det alltid viktigt att kontrollera att dina krav och behov möts av leverantören. Det är du som måste säkerställa att dina behov tillgodoses, att era processer fungerar tillsammans och är kompatibla och att dina risker hanteras enligt dina behov och i enlighet med gällande lagstiftning.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Upphovsrätt och begränsningar:

Om eventuell information från IDC eller referenser till IDC ska användas i annonser, pressmeddelanden eller marknadsföringsmaterial krävs ett skriftligt tillstånd från IDC. Om du har frågor om sådana tillstånd kan du kontakta Custom Solutions på 508-988-7610 eller ermissions@idc.com. För översättning och/eller lokalisering av det här dokumentet krävs en ytterligare licens från IDC. Mer information om IDC finns på www.idc.com. Mer information om IDC Custom Solutions finns på http://www.idc.com/prodserv/custom_solutions/index.jsp.

Globalt huvudkontor: 5 Speen
Street Framingham, MA 01701
USA P.508.872.8200
F.508.935.4015 www.idc.com.

Copyright 2019 IDC. Kopiering
förbjuden utan tillstånd. Med
ensamrätt.

Om IDC

International Data Corporation (IDC) är den främsta globala leverantören av marknadsanalyser, rådgivningstjänster och evenemang inom IT, telekom och konsumentteknik. IDC hjälper IT-experter, företagsledare och investerare att fatta faktabaserade beslut om teknikinköp och affärsstrategier. Fler än 1 100 IDC-analytiker i över 110 länder tillhandahåller global, regional och lokal expertis om teknik, marknadsmöjligheter och trender. I 50 år har IDC tillhandahållit strategisk information i syfte att hjälpa våra kunder att uppnå sina viktigaste affärsmål. IDC är ett dotterbolag till IDG, världens ledande företag inom teknikmedia, undersökningar och evenemang.