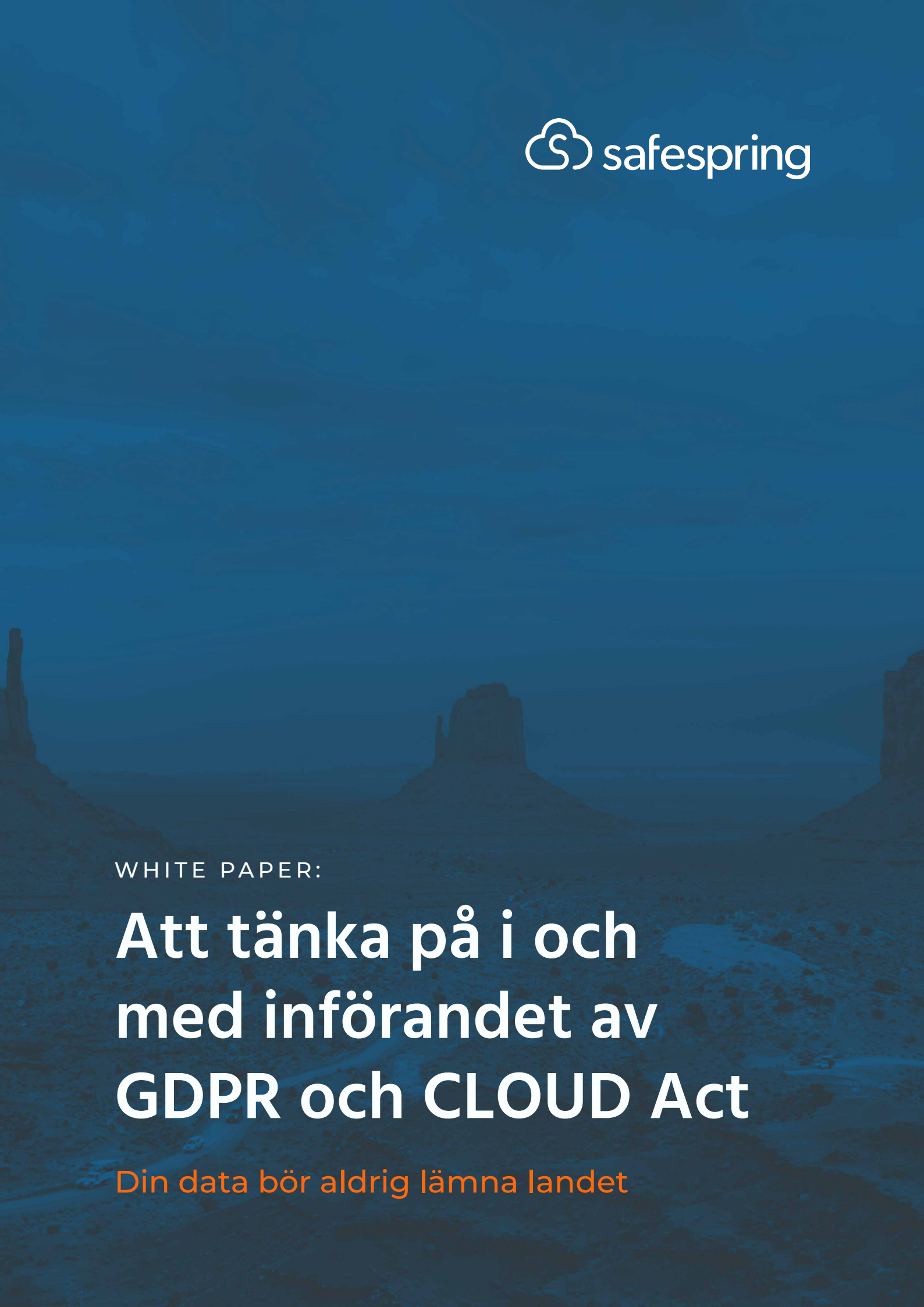

WHITE PAPER:

Att tänka på i och med införandet av GDPR och CLOUD Act

Din data bör aldrig lämna landet


Foto: David Larencranz

Inledning

Detta white paper handlar om EUs- och amerikansk rätts bestämmelser om gränsöverskridande dataöverföringar samt aktuella rättsfall som kan komma påverka detta.

Allmänna dataskyddsförordningen (eng: GDPR) trädde i kraft den 25:e maj 2018 och ersätter Personuppgiftslagen (PUL). Den är varken början eller slutet på EU:s sedan länge pågående ansträngningar att förbättra skyddet av individens data samt rätt till privatliv. Dessa rättigheter är grundläggande mänskliga rättigheter i EU och samtliga medlemsstater är bundna av dem på områden som faller under EU:s kompetens i och med ikraftträdandet av Lissabonfördraget 20091. EU förstärker därmed sitt försprång över USA när det gäller rättsliga skydd för individers rätt till privatliv och data.

Bakgrund

Dataskyddsdirektivet[2] från 1995 skapade ett EU-gemensamt regelverk för skydd av personuppgifter.

Det var fortfarande upp till vart enskilt land att införa nationell lagstiftning utifrån direktivet. I Sverige genomfördes direktivet i nationell rätt 1998 genom personuppgiftslagen (PUL)[3]. PUL reglerade dels vilka sorters personuppgifter som fick registreras samt även hur dessa fick överföras till så kallat "tredje land". Det senare krävde att åtminstone en av tre följande situationer gällde:

1) Landets personuppgiftslagstiftning anses jämförbar med den europeiska (33 § PUL)
2) Individen har gett samtycke eller har genom ingående av kontrakt de facto accepterat viss utlämning (34 § PUL),
3) Regeringen har särskilt meddelat undantag (35 § PUL).

GDPR till skillnad från Dataskyddsdirektivet gäller som EU-lag direkt, och kräver inte omsättning av EU-reglerna i nationell lagstiftning. Det medför att samtliga EU-medlemsstater nu har fått en ännu mer harmoniserad lagstiftning vad gäller personuppgiftsskydd. Mindre lokala anpassningar av vissa detaljer i GDPR tillåts, särskilt vad gäller offentlig förvaltning, men den stora merparten av lagstiftningen förblir lik medlemsländer emellan.
Det fanns fram till 6:e oktober 2015 ett flertal sätt att möjliggöra överföring till tredje land, varav de tre huvudsakliga alternativen till överföring var:

1) **SAFE HARBOR**[4] - system för amerikanska bolag att själv-certifiera sin personuppgiftshantering,
2) **BINDING CORPORATE RULES** - riktlinjer och processer för multinationella företags interna överföringar, och
3) **STANDARD CONTRACT CLAUSES**[5] - ett standardkontrakt som en europeisk kund kan teckna med amerikansk leverantör.

Den 6:e oktober 2015 ogiltigförklarade Europa-domstolen i C-362/14 EU-kommissionens beslut om Safe Harbor[6]. Den andra februari 2016 beslutade EU-kommissionen på nytt om ett system för amerikanska bolag att själv-certifiera sig, det s.k Privacy Shield.[7]

Vid sidan av personuppgiftsskyddet som gäller vid interaktioner mellan enskilda och företag eller enskilda och myndigheter finns ett särskilt system för dataöverföring i verksamheter som rör brottsbekämpande myndigheter. Dessa myndigheter kan inhämta information i förundersökningar och liknande från andra länder via så kallade MLAT-avtal (Mutual Legal Assistance Treaty).

Aktuellt

Idag kan amerikanska IT-bolag tvingas lämna ut persondata när amerikanska myndigheter så kräver, oavsett fysisk plats där denna data befinner sig.

CLOUD Act

Clarifying Lawful Overseas Use of Data Act (US CLOUD act)[8] är en amerikansk lag som röstades igenom den 23:e mars 2018, med syfte att undanröja tidigare hinder i den amerikanska lagstiftningen för amerikanska IT-bolag att lämna ut persondata när amerikanska myndigheter så kräver, oavsett fysisk plats där denna data befinner sig.

Lagen innehåller också en process där den amerikanska regeringen kan kvalificera andra länder att få lov att begära data från amerikanska bolag. Ett ytterligare syfte med lagstiftningen är att kringgå idag existerande MLAT (se ovan), bland annat därför att MLAT-processer anses långsamma. MLAT-processer innefattar att begäranden om utlämnande av uppgifter granskas av domstolar, vilket tar tid[9]. Såväl europeiska som brittiska representanter inom brottsbekämpning har varit i förhandling med amerikanska motsvarigheter för att förbättra situationen inom området och få till stånd enklare och snabbare tillgång av utländsk sparad data i brottsmålsundersökningar.

När *Microsoft vs US Government*[10] hade tagits upp i amerikanska Högsta Domstolen under våren 2018 fick den amerikanska sidan bråttom att införa ny lag för att undvika att det förväntade domslutet, tills lagen ändrades, skulle cementera ett utfall som varken Microsoft eller US Government (MS-vs-USG) önskade[11]. Lagstiftningen i sig är hastigt[12] framtagen och har fått en mängd kritik av olika skäl, bland annat en oro för att icke-amerikanska myndigheter ska kunna komma åt olämplig data via de bilaterala samarbetsavtalen[13], men även på juridiskt plan då applicerandet av extraterritoriell lagstiftning är en snårskog[14]. Fallet i Högsta Domstolen lades ner efter att US CLOUD Act blev fastslagen[15].

Irland[16] såväl som EU-kommissionen[17] har gjort så kallade amicus curiae-inlagor[18] i MS-vs-USG, som sammanfattningsvis i det senare fallet konstaterar att EU har ett intresse av internationellt rättskipande samarbete, men samtidigt att all form av utlämning av data fysiskt lagrad i EU måste ske i enlighet med GDPR för att vara laglig i EU[19]. I GDPR är det särskilt Artikel 48[20] som behandlar verkställande av tredjelands domstols- eller myndighetsbeslut inom EU, och säger att sådan överföring "*endast får genomföras om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp* [eng: MLAT]". Irland samt EU-kommissionen pekar bägge i sina inlagor på att den rimligaste vägen är just de redan existerande MLAT-avtalen.

US CLOUD Act har alltså ännu inte förändrat det grundläggande läget: amerikansk europeisk rätt är inte kompatibla i frågan om utlämning av data sparad i EU till USA. Tills avtal mellan EU eller mellan var och en av medlemsstaterna och USA finns på plats som legaliserar användningen av US CLOUD Act gentemot Artikel 48 i GDPR, är det enda tillåtna sättet som harmoniserar med europeisk rätt, att USA använder sig av de existerande MLAT-avtalen, vilket var det USA önskade komma ifrån i första läget.

Det finns alltså framförallt tre frågor som spelar en avgörande roll framåt vad gäller US CLOUD Acts inverkan på amerikanska IT-bolags verksamhet inom EU:

1) Kommer EU och USA, eller var och en av medlemsstaterna och USA, att få ett eller flera avtal på plats som gör det amerikanska användandet av US CLOUD Act lagligt ur ett europeiskt perspektiv?

2) Kommer ett sådant avtal att leva upp till Stadgan för grundläggande rättigheter (EU-stadgan)?

3) Kommer USA att respektera europeisk territorialitet för GDPR eller kommer överföringar att ske i strid mot GDPR och kommer EU att ha insyn i detta, eller agera om sådan överföring upptäcks?

I EU-domstolsbeslutet i "Safe Harbor"-fallet resonerar domstolen inte i första hand i termer av vad som bevisligen har skett i enskilda fall, utan, vad amerikansk lag de facto möjliggör. Gällande den tredje punkten ovan så möjliggör US CLOUD Act för USA att begära överföring av data i strid mot GDPR: Det är enligt US CLOUD Act upp till det tillfrågade bolaget att på eget initiativ opponera sig i domstol - en amerikansk domstolsprocess sker endast då. Även om den amerikanska domstolen skulle finna skäl mot att godkänna en begäran om utlämning av data, kan den också finna skäl för att godkänna det. Det är explicit inskrivet i lagen ett antal områden som domstolen behöver ta ställning till, däribland amerikanska intressen inklusive nationella säkerhetsintressen. Ur ett europeiskt perspektiv blir detta besvärligt. Den europeiska rätten till dataskydd skyddar europeiska medborgare, och det europeiska rättsväsendet (särskilt domstolarna) har till uppgift att se till att europeisk lagstiftning tolkas så att den skyddar europeiska medborgare.

Det man måste förstå är att EU-stadgan tillhör ramfördragen, och avser kodifiera EU:s grundprinciper. Det betyder att annan EU-rätt som direktiv, förordningar, och regler för avtal, successivt bygger ovanpå den lagstiftningen. EU-stadgan garanterar rättigheter till EU-medborgare, som europeiska domstolar måste förhålla sig till vid rättstvister. Det ser därför ut som att den andra frågan ovan leder till samma grundläggande frågeställning som EU-domstolen redan måste ta i beaktande i och med hanteringen av fallet "Data Protection Commissioner" (se nedan). Andra punkten kan också sägas till stor del redan ha bedömts i C-362/14 (se särskilt paragraf 79-98 som fullständigt fällde Safe Harbor-avtalet).

När det gäller den första frågan hävdas det att Storbritannien ligger i bilaterala förhandlingar med USA i syfte att få till stånd ett nytt MLAT-avtal[21], medan EU eftersträvar ett multilateralt avtal för hela unionen med USA[22]. Ett problem för EU är att US CLOUD Act strikt läst inte tillåter att USA ingår multilaterala avtal snarare än bilaterala avtal, vilket kan innebära att amerikansk lag förhindrar amerikanska staten från att göra annat än att söka bilaterala avtal med varje enskilt EU-medlemsland. För EU vore en sådan lösning otillfredställande. Ytterligare lagstiftning eller en "snäll" tolkning av US CLOUD Act krävs för att EU ska kunna söka ett multilateralt avtal.

C-311/18, Data Protection Commissioner

Efter Safe Harbor-beslutet ogiltigförklarades av EU-domstolen den 6:e oktober 2015 i C-362/14 ansökte österrikaren Max Schrems igen till den irländska datainspektionen om tillsyn av Facebook Irlands dataflöden ut ur EU. Han menade att det, givet utfallet i C-362/14 omöjligen kunde vara tillåtet att överföra data till USA baserat på Standard Contract Clauses eller Privacy Shield. Fallet gick till domstol då Schrems argumenterade för att den irländska datainspektionen själva kan besluta om att stoppa Facebooks dataflöden ut ur EU. USA:s regering, Digital Europe, the Business Software Alliance bistår Facebook i fallet, medan Schrems och den irländska datainspektören bistås av EPIC.

Datainspektören håller med Schrems om att EU-stadgans artikel 47 -- *Rätt till ett effektivt rättsmedel och till en opartisk domstol* -- inte respekteras i den ordningen som etableras av Standard Contract Clauses och Privacy Shield, samt om risken för att EU-medborgares rättigheter enligt artikel 7 och 8 därmed är hotade. Den irländska High Court[24] beslöt den 3:e oktober 2017 att hänvisa ärendet till EU-domstolen så att domslutet blir giltigt i hela EU. Facebook överklagade beslutet att hänvisa till EU-domstolen till den irländska Supreme Court. När High Court väl annonserade själva hänvisningen den 12:e april 2018 ansökte sedan Facebook till High Court om att frysa hänvisningen till EU-domstolen i väntan på beslut av Supreme Court. High Court beslutade den 2:a maj emot detta då Facebooks ansökan saknade grund, och skrev att "hänvisningen måste fortsätta omedelbart", samt att Facebooks agerande i domstolen har varit på gränsen till klandervärt och oseriöst[25]. Medias bedömning är att Facebook på olika vis försöker försena rättsprocessen[26]. Det var tydligt även i den utfrågning som EU-parlamentet genomförde den 22:a maj 2018 med Facebooks VD, Mark Zuckerberg, att Facebooks affärsverksamhet har en mängd aktuella konfliktzoner med EU[27 28 29]. En EU-parlamentariker konstaterade under utfrågningen med Zuckerberg nivåskillnaderna mellan USAs och EUs dataskydd och svårigheten att förena dessa två[30]. Giltigheten av både Standard Contract Clauses samt Privacy Shield ifrågasätts i hänvisningen till EU-domstolen. När det gäller Privacy Shield gäller tvisten i första hand om den Ombudsperson som USA:s regering tillsätter uppfyller EU-rättens krav på en oberoende rättsinstans med ett antal ytterligare egenskaper. När man läser paragraf 43 och 44 i hänvisningen är det svårt att se hur detta skulle kunna vara fallet givet det resonemang som den irländska datainspektionen har fört, men vi får vänta på EU-domstolens beslut.

Hänvisningen består av 11 st frågor som ber EU-domstolen att uttala sig om Standard Contract Clauses samt Privacy Shield är förenliga med unionsrätten (EU-stadgan, etc) men det finns inte utrymme att beskriva samtliga övriga inledande frågor här. Man bör känna till att EU-domstolen ibland svarar på frågor de önskar de hade fått, snarare än frågorna de faktiskt fick, varför man inte skall förvänta sig några raka svar.

Slutsats

Givet ovan beskrivna rättssituation med den stora diskrepans som finns mellan utformningen på amerikansk lag och rätt kontra europeisk dito är det svårt att se hur de bägge regimerna är förenliga sinsemellan.

FÖR DET FÖRSTA finns det inga indikationer på att europeiska domstolar kan tänka sig att kraftigt försämra sådana medborgerliga rättigheter som lagfästs. Den möjligt framkomliga riktningen är att amerikansk lag förbättrar skyddet för enskilda. En sådan utveckling skulle dock gå tvärtemot amerikansk praxis gällande just nationell säkerhet, som i praktiken inte erkänner sådana personers rättigheter som inte är medborgare i USA (vilket ju EU-medborgare typiskt inte är), vilket uttalanden av rättsexperter i High Courts hänvisning till EU-domstolen C-311/18 gör gällande.

FÖR DET ANDRA är det möjligt att EU-domstolen kommer ogiltigförklara både Standard Contract Clauses samt Privacy Shield, och att EU-kommissionen förhandlar fram ett "Safe Harbor 3" med USA, i den utsträckning US CLOUD Act inte gjort ett sådant omöjligt. Man kan spekulera i vilken parts position som stärks mest inför förhandlingarna av ett sådant beslut från EU-domstolen.

FÖR DET TREDJE finns det för närvarande en politisk situation mellan EU och USA som är allt annat än god. Baksidorna av amerikanska IT-bolags integritetspolicies, som t.ex. Facebook, som delvis anses ha gjort Brexit möjligt genom påverkanskampanjer, har inte gått EU-politiker förbi. Till detta kan läggas diplomatiska problem som har uppstått i och med att USA dragit sig ur Iran-avtalet, och det begynnande handelskrig som USA:s regering har skapat.

FÖR DET FJÄRDE är en vanlig invändning mot att EU-domstolen skulle kunna ogiltigförklara både Standard Contract Clauses samt Privacy Shield alls, eller utan att ett alternativ finns på plats, att det skulle ha så stora konsekvenser på affärsverksamhet. EU-domstolens uppgift är att se till att EU-stadgan efterlevs i EU:s lagar och beslut. Om EU-stadgan är i vägen för affärsverksamhet behöver den i så fall ändras på. Tills dess gäller den som den är. EU-kommissionen har konstaterat att europeiska medborgares rättigheter blev kränkta men ansåg sig inte nödgade att ändra på Safe Harbor-beslutet i ljuset av detta, i väntan på en stundande omförhandling av beslutet med USA. EU-domstolen å sin sida hävdar att man tvärtom faktiskt bör stoppa överföringarna vid ett sådant konstaterande för att sluta kränka EU-medborgares grundlagsskyddade rättigheter[31].

VAD NÄSTA STEG SKULLE BLI efter att EU har ogiltigförklarat USA som adekvat tredje land kan man bara spekulera om. Man kan dock konstatera att vid EU-domstolens förra förhandsavgörande i C-362/14 upphörde Safe Harbor omedelbart att gälla, men de europeiska datainspektionerna gav personuppgiftsombud (biträde) 3 månaders respit så att EU-kommissionen och USA skulle kunna hitta en ny lösning. Om inte en ny lösning står att finna i närtid, behöver personuppgiftsombud upphöra med behandling av personuppgifter på drabbade tjänster för att undvika hot om böter.

Rekommendationer till organisationer

Givet rättssituationen finns några strategiska rekommendationer, gällande molntjänster, för att undvika att hamna i kläm innan (eller om inte) de rättsliga motstridigheterna mellan EU och USA har retts ut.

Rekommendationer: IT-arkitektur

1) Se till att bygga molninfrastrukturen med agnostiska verktyg och plattformar för att enklare kunna flytta miljön till en annan leverantör om det rättsliga läget förvärras. Att bygga sin miljö med containrar (eller Docker) istället för virtuella servrar är ett beprövat sätt som underlättar migrering av tjänsterna till en annan leverantör.
2) Räkna på hur dataöverföringskostnaderna skulle slå den dagen ni vill flytta ut. Många molntjänsteleverantörer tar inget betalt för att lägga upp - men desto mer för att hämta hem vilket kan ge obehagliga överraskningar.
3) Se till att separera datat från tjänsterna med öppna (eller åtminstone standardiserade) gränssnitt för enklare kunna byta datalagringsplattform. Amazons S3-protokoll har blivit branschstandard för storskalig lagring av ostruktuerad data i molnet. Dessvärre använder Amazon sig av vissa tillägg som inte stöds av andra S3-kompatibla tjänster. Om man ser till att använda sig av en mer generisk S3-kompatibel leverantör i första läget så är det enklare att flytta till en annan leverantör.
4) Investera i en egen identitetshantering istället för att lita på molntjänst-leverantörens. Detta kommer i vissa fall bli lite krångligare men otroligt mycket enklare om tjänsterna skall migreras någon annanstans.

Rekommendationer gällande riskanalys och tillmötesgående av personuppgiftsskyddslagstiftning

1) Gör grundarbetet med GDPR kring hantering av personuppgifter. Ett sådant grundarbete bör inkludera att man ser över:
   - **a)** var man geografiskt lagrar sina personuppgifter,
   - **b)** vad man har för laglig grund för behandlingen samt (om personuppgifterna lagras utanför EU/EES) för själva överföringen dit,
   - **c)** hur känsliga personuppgifter det är som behandlas (särskilt om det sker utanför EU/EES),
   - **d)** om man informerat de registrerade individerna i fråga om att deras personuppgifter behandlas, och
   - **e)** om det finns någon gallringsrutin implementerad. Denna punkten är förstås särskilt viktig om uppgifterna lagras i USA eftersom organisationer då i alla fall har ett naturligt sätt att minska de uppgifter som skulle kunna komma att behöva lämnas ut.
2) Fördjupa GDPR-arbetet med att införa säkerhetsklassning av den information som behandlas inom organisationen -- detta är nödvändigt för att därefter kunna göra korrekt lämplighets- och riskanalys kring användandet av olika molntjänster
3) Inkludera i riskanalysen den legala osäkerheten kring existerande och nya molntjänstleverantörer -- gör en sannolikhetsbedömning och konsekvensanalys och agera utifrån detta: Om det antas till exempel vara 20% risk för ett fullt stopp av överföring av personuppgifter till amerikanska tjänster under 12 månader med start om 9 månader, hur skulle detta påverka verksamheten och beslutsprocessen kring IT-strategi gällande val av leverantörer?
4) Ha redundans även av leverantörer. Särskilt viktigt för tjänster i riskzonen och gör en bedömning kring migrationsprocessen -- hur lång tid tar det t.ex. att byta ut samtliga amerikanska tjänster om behovet skulle uppstå? Det kan tyckas för katastrofalt för att ens övervägas men underlaget behövs för att kunna ta rätt beslut om det skulle bli skarpt läge.

Läs mer om våra tjänster

Besök gärna vår webbplats för att lära dig mer om molntjänster och hur Safespring kan lösa era Backup-, Lagrings- och infrastrukturbehov.

www.safespring.com

safespring

+46 (0)8-55 10 73 70 | info@safespring.com
Smidesvägen 12, 171 41 Solna, Sweden

www.safespring.com

Källförteckning

Detta White Paper är skrivet av Martin Millnert för Safespring. Safespring erbjuder svenskproducerade molntjänster där data aldrig lämnar landet.

1) Stadgan för grundläggande rättigheter
2) Europaparlamentets och rådets direktiv 95/46/EG 1995
3) Personuppgiftslagen (PUL)
4) Safe Harbor Privacy Principles
5) Standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland
6) C-362/ 14 Schrems v Data Protection Commissioner, EU:C:2015:650
7) Skölden för skydd av privatlivet i EU och Förenta staterna
8) Clarifying Lawful Overseas Use of Data Act
9) James Scott, Co-Founder & Sr. Fellow, ICIT
10) Ett mångårigt rättsfall som i grunden handlar om att USA:s "Stored Communications Act" ej tillåter amerikanska IT-bolag att lämna ut data sparad utanför USAs territorium till amerikanska myndigheter.
11) Albert Gidari - The Center for Internet and Society at Stanford Law School
12) Nikolaj Nielsen - EU Observer
13) Katitza Rodriguez - Electronic Frontier Foundation
14) Gavc Law – Veert van Calster
15) 17-2 United States v. Microsoft Corp. (04/17/2018)
16) Ireland - Amicus Brief
17) Microsoft Word - Draft Amicus Brief in US v Microsoft
18) Inlägg i pågående domstolsfall av icke-parter för att förse domstolen med mer relevant fakta.
19) Lee Matheson, CIPP/E, CIPP/US, CIPM
20) Dataskyddsförordningen
21) The Register - Independent news and views for the tech community
22) Catherine Stupp - EURACTIV.com
23) Data Protection Commissioner v. Facebook Ireland Limited & Schrems
24) Mary Carolan - The Irish Times
25) The High Court Judgement - Irland
26) Aodhan O'Faolain - Independent
27) Stephanie Bodoni - Bloomberg
28) Sara Salinas - CNBC
29) Ryan Browne - CNBC
30) EP Conference of Presidents with Mark Zuckerberg
31) Mål C-362/14 - Maximillian Schrems mot Data Protection Commissioner