En bilaga till Swecos digitaliseringsblogg

Förtydliganden av de 6 steg som EDPB tagit fram för att kunna använda molntjänster eller överföra uppgifter till tredjeland

Steg 1 : Kartlägg dina överföringar

- Analysera och kartlägg vilka överföringar som genomförs från ditt företag till tredje land. Detta omfattar vilka överföringar som sker genom personuppgiftsbiträden, underbiträden och vidare från dem.
- Använd ditt Artikel 30-register (registerförteckning) som utgångspunkt för att identifiera behandlingar där överföring till tredje land eller internationell organisation kan förekomma.
- Tänk på att distansåtkomst från ett tredjeland (exempelvis en helpdesk eller supportverksamhet) också räknas som en överföring. Molntjänster där infrastrukturen för molntjänsten finns i tredjeland blir också en överföring.
- Om du använder en molntjänst som tillhandahålls av en internationell molntjänstleverantör behöver du veta var de har sitt säte och hur mycket av bolaget som ägs av ett internationellt bolag, då detta också kan ha bäring på om de så kallade besvärande lagstiftningarna nedan kommer att träffa bolaget.
- Bara om molntjänstleverantören är helt etablerad och har sitt säte inom EU/EES (inkl. moderbolag) och det tydligt framgår att personuppgifter inte kommer att överföras till tredjeland kommer du att kunna använda molntjänsten utan att det klassas som en överföring till tredjeland eller internationell organisation.

Steg 2: Identifiera överföringsmekanism

Kapitel V i dataskyddsförordningen anger specifika fall och scenarion där överföring är tillåten:

Adekvat skyddsnivå (artikel 45)

Om överföringen sker till en mottagare (importör) som finns i ett av länderna som EU-kommissionen har bedömt uppfyller samma skyddsnivå som inom EU/EES kan överföring kan ske utan att ta till ytterligare lämpliga skyddsåtgärder som krävs enligt artikel 46 i dataskyddsförordningen.

Lämpliga skyddsåtgärder (artikel 46)

För det fall tredje landet inte uppfyller adekvat skyddsnivå kan det gå att överföra uppgifter om man kan vidta andra lämpliga skyddsåtgärder, vilket omfattar:

- EU-kommissionens godkända standardavtalsklausuler (SCC – Standard Contract Clauses), vilka inte får lov att ändras för att de ska vara giltiga.
- Bindande företagsbestämmelser (BCR – Binding Corporate Rules) vilka ska godkännas av EDPB lista finns på EDPB:s hemsida Approved Binding Corporate Rules
- bindande överenskommelser mellan offentliga myndigheter eller organ
- godkända uppförandekoder (godkända enligt artikel 40)
- en godkänd certifieringsmekanism (enigt artikel 42)
- övriga avtalsklausuler mellan parterna som möjliggör överföring där kraven som åligger mottagaren (importören) motsvarar kraven i dataskyddsförordningen och går att verkställa i praktiken.

Oavsett vilken överföringsmekanism som väljs måste exportören och personuppgiftsansvarig säkerställa att personuppgifterna får samma skydd som ges av dataskyddsförordningen.

Undantag i särskilda situationer (Artikel 49)

Det finns särskilda situationer listade i denna artikel som möjliggör överföring (kortfattade beskrivningar):

- den registrerade har lämnat sitt samtycke (observera kraven som behöver uppfyllas för att ett samtycke ska anses vara giltig).
- överföringen är nödvändig för att fullgöra ett avtal eller åtgärder som föregår ett avtal
- överföringen är nödvändig för att ingå eller fullgöra ett avtal i den registrerades intresse
- överföringen är nödvändig av viktiga skäl som rör allmänintresset.
- överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk

Men **observera** att strikta krav behöver uppfyllas för att kunna använda något av dessa situationer. EDPB har tagit fram Riktlinjer 2/2018 för undantagen i artikel 49 som stöd i utvärderingen. Notera att överföringar som är möjliga genom artikel 49 omfattar normalt inte överföringar som sker kontinuerligt och regelbundet utan är avsedda för särskilda specifika situationer och överföringar.

Steg 3: Utvärdera överföringsmekanismen under artikel 46

Identifiera lag och praxis, dataskyddslagstiftning eller problematisk lagstiftning i tredje landet som är relevanta för just din överföring

Kan mottagarlandets lagstiftning ge samma rättigheter och skydd som dataskyddsförordningen? Exempel på detta kan vara:

- att en EU medborgare inte har samma rättigheter i mottagarlandet som de egna medborgarna
- det finns inte någon reglering för dataskydd som motsvarar dataskyddsförordningen
- det finns lagar som möjliggör åtkomst till personuppgifter som överförs eller behandlas i mottagarland

Resultatet av utvärderingen av lagstiftningen och riskerna förknippade med det hjälper dig att identifiera vilka ytterligare skyddsåtgärder som behövs i steg 4.

Steg 4 : Identifiera och vidta kompletterande skyddsåtgärder

Kompletterande skyddsåtgärder kan vara en kombination av tekniska, avtalsmässiga och organisatoriska åtgärder som tillsammans uppnår ett likvärdigt skydd för den registrerade.

Identifiera och anta skyddsåtgärder för att komma upp till samma nivå som EU:s dataskyddsförordning. Detta kan vara att:

- Ingå avtal som innehåller EU godkända standardavtalsklausuler
- Säkerställa tekniska åtgärder så som kryptering, pseudonymisering, uppdelning av uppgifter
- Kan ni minimera personuppgifterna som överförs (både i typ och omfattning)

Steg 5: Praktiska steg om du har identifierat effektiva kompletterande skyddsåtgärder

Vid användning av tekniska skyddsåtgärder säkerställ att de inte går emot SCC. Tillstånd från tillsynsmyndighet behövs om man gör avsteg från de EU godkända standardavtalsklausulerna (SCC).

Steg 6: Omvärdera riskerna och skyddsåtgärderna med lämpliga mellanrum

Övervaka förändringar i lagstiftning och praxis i tredjelandet och EU, utveckling inom tekniken eller övrigt i omvärlden som kan leda till att du behöver omvärdera och ändra åtgärderna som har vidtagits. Det kan innebära att överföringen kan behöva upphöra under tiden en ny utvärdering görs.

Lagstiftningar att ha koll på

US Cloud Act (Clarifying Lawful Overseas Use of Data)

Denna amerikanska lagstiftning från 2018 kan träffa organisationer som har sitt säte i USA även om verksamheten eller lagring finns inom EU/EES. Denna lagstiftning gör det möjligt för amerikanska myndigheter att via juridisk process beordra tjänsteleverantörer (exempelvis telekomoperatörer eller molntjänstleverantörer) att lämna ut specifika uppgifter om personer (både direkta och indirekta uppgifter) även om uppgifterna behandlas inom EU/EES.

Trots att det finns möjligheter för en tjänsteleverantör att begära överprövning av ett Cloud Act-beslut så är grunderna för överprövning begränsade och i praktiken är det oklart om någon tjänsteleverantör kommer att göra detta.

Med Cloud Act kan myndigheter i USA kringgå annan ömsesidig rättshjälp som finns genom den europeiska MLAT (Mutual legal assistance in criminal matter treaty) som gäller mellan USA och EU vilket är mellanstatligt och därför främst kan beröra statliga myndigheter.

Dock har EDPB & EDPS i sin opinion i juli 2019 om US Cloud Act tydliggjort att artikel 48 GDPR endast möjliggör utlämning om det är med stöd av annan överenskommelse mellan EU/EES medlemslandet och tredjelandet (som MLAT). Ett domstolsbeslut utgör inte i sig själv stöd för utlämnande och behöver stöd från internationell överenskommelse för att en utlämning ska vara tillåtet utifrån Artikel 48. Därför kommer tjänsteleverantören som lämnar ut uppgifter att göra detta i strid med GDRP. Det enda möjliga exceptionella undantaget kan vara där ett utlämnande är för att skydda den enskildes vitala intressen (dvs. liv och hälsa).

Så om en tjänsteleverantör kommer att bryta mot GDPR om de lämnar ut uppgifterna finns där i så fall något som tyder på att de kommer att lämna ut uppgifterna? Om de inte lämnar ut uppgifterna kommer de i så fall att gå emot ett domstolsbeslut i USA och detta kan också medföra konsekvenser för tjänsteleverantören, så det blir förmodligen en fråga om vad som väger tyngre för just den tjänsteleverantören och konsekvenserna om den bryter mot GDPR eller Cloud Act. Det får tiden utvisa, men det blir personuppgiftsansvarig som i slutändan tar risken om de bryter mot GDPR.

FISA 702 (FISA Amendments Act of 2008 Section 702)

Ytterligare en besvärande amerikansk lagstiftning som kan träffa behandling av personuppgifter för en EU-medborgare är FISA 702. Detta eftersom den möjliggör, utan domstolsbeslut, och oavsett annan lagstiftning, att chefsjurist (Attorney General) kan godkänna inhämtning av underrättelseinformation om icke-amerikaner som befinner sig utanför USA. Det möjliggör insamling via övervakning av den fysiska infrastrukturen hos amerikanska företag som tillhandahåller elektroniska kommunikationstjänster (detta kan vara e-posttjänster, molntjänster). Eftersom denna lagstiftning träffar amerikanska företag så innebär det att leverantörer som har sitt säte i USA kan bli tvingade att lämna ut information även om utrustning och kommunikation samt data finns inom EU/EES. Informationen kan dessutom lämnas vidare till andra brottsbekämpande myndigheter så som CIA och FBI. Den nationella underrättelsetjänstens stab har tagit fram en förklarande infographic som ger en överblick av hur lagstiftningen tillämpas.

Även EDPB tar upp FISA 702 i sina riktlinjer för kompletterande skyddsåtgärder (se sida 20) vid tredjelandsöverföringar och poängterar att den inte ger skydd för den registrerad som motsvarar EU lagstiftningen.

Det som är svårt att överblicka är risken för att information kommer att begäras ut och huruvida ett företag har möjlighet att neka eller ens kunna berätta om att en begäran har mottagits.