

Viktiga förändringar för överföring av personuppgifter utanför EU/EES

Information till nämnder och bolag i Region Västerbotten med anledning av Schrems II-målet

Bakgrund

Vid överföring av personuppgifter till länder utanför EU/EES, s.k. tredjeland, är utgångspunkten att detta endast är tillåtet om det kan garanteras att det land som är mottagare eller som får tillgång till personuppgifterna har en tillräckligt hög skyddsnivå. Detta förutsätter att det finns ett likvärdigt skydd för personuppgifter som inom EU. Tidigare har organisationer kunnat hänvisa till Privacy Shield (USA och Kanada) och SCC – standardavtalsklausulerna (övriga länder), men det har i ett nytt avgörande från EU-domstolen konstaterats att skyddet från dessa inte är tillräckligt.

Schrems II-målet

Den 16 juli meddelade EU-domstolen dom i det s.k. Schrems II-målet, ett av de allra mest betydelsefulla avgörandena från EU-domstolen på personuppgiftsområdet. Genom domen ogiltigförklaras Privacy Shield, vilket direkt medför stora konsekvenser för överföring av personuppgifter till USA och Kanada.

Domstolen förtydligar dessutom under vilka förhållanden standardavtalsklausuler kan användas för överföring av personuppgifter utanför EU/EES. Den som vill använda sig av sådana måste, innan överföringen genomförs, säkerställa att nivån av dataskydd i standardavtalsklausulerna kan respekteras i det land där mottagarparten befinner sig. Detta innebär att standardavtalsklausulerna inte kommer kunna användas lika enkelt som innan.

EU-domstolen anser att det skydd som ges i Privacy Shield är för svagt och att amerikanska myndigheter har för stora möjligheter att få åtkomst till personuppgifter, särskilt mot bakgrund av de övervakningsprogram som genomförs av den amerikanske staten. Sammanfattningsvis gör domstolen bedömningen att överföringarna inom ramen för Privacy Shield utgör en för stor risk för att rättighetsskyddet för enskilda enligt EU-rätten kränks.

Standardavtalsklausulerna ogiltigförklaras inte av EU-domstolen i målet, men domstolens resonemang avseende de krav som ställs för att kunna använda dem i praktiken skapar osäkerhet kring i vilken utsträckning de kan användas för överföringar till USA, särskilt mot bakgrund av EU-domstolens resonemang angående USA:s övervakningsprogram och skyddet för personuppgifter i landet. EU-domstolen poängterar också att de europeiska tillsynsmyndigheterna har en skyldighet att förbjuda överföring med hjälp av standardavtalsklausulerna till länder som inte erbjuder tillräckligt skydd för personuppgifter.

Domen innebär alltså i korthet att:

- Privacy Shield har ogiltigförklarats. Det inte längre är möjligt att förlita sig på certifieringen för överföring av personuppgifter till USA eller Kanada, vilket kraftigt begränsar möjligheten att överföra personuppgifter till dessa länder.
- Organisationer som använder sig av standardavtalsklausulerna för överföring av personuppgifter måste verifiera om klausulerna respekteras i mottagarlandet och om några extra säkerhetsåtgärder krävs.

Juridik och säkerhet
Tobias Lindberg

2020-09-29

395646

Exempel på lämpliga extra säkerhetsåtgärder framgår inte av domen. Förhoppningsvis finns vägledning från tillsynsmyndigheterna inom kort. Den Europeiska dataskyddsstyrelsen ("EDPB") har erbjudit hjälp till EU-kommissionen och USA att hitta och bygga ett nytt ramverk för överföringar mellan EU och USA. Utan ytterligare vägledning är risken stor att överföringar till USA inte kommer kunna ske.

Hur påverkar detta oss?

Det är respektive nämnd, styrelse eller bolag i regionen som är personuppgiftsansvariga och därmed har det yttersta ansvaret för personuppgiftsbehandlingarna. Den personuppgiftsansvarige ska genomföra tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Det är alltså respektive nämnds eller bolags ansvar att säkerställa att alla överföringar utanför EU/EES (exempelvis till USA) är lagliga.

Regionen har olika samarbetspartners (personuppgiftsbiträden) som har servrar och/eller personal utanför EU/EES. Det är sannolikt att flera av dessa avtal baseras på Privacy Shield eller standardavtalsklausulerna. Dessa avtal behöver inledningsvis kartläggas och eventuellt omförhandlas så att personuppgifterna endast behandlas inom EU/EES. En annan lösning är att ingå standardavtalsklausuler samt säkerställa att klausulerna kommer att respekteras i mottagarlandet genom att eventuellt införa ytterligare säkerhetsåtgärder.

Vad måste vi göra nu?

Nämnder och bolag bör omgående ta hänsyn till konsekvenserna av domen i samband med tecknande av nya avtal och i upphandlingar. Avtal som innefattar behandling av personuppgifter bör inte tecknas med aktörer som har servrar eller personal utanför EU/EES. Undantag från detta bör ske mycket restriktivt och enbart i situationer där andra alternativ helt saknas och skyddet för personuppgifter grundligt utreds och dokumenteras innan avtalet ingås.

Vägen framåt

Dataskyddsombudet lämnar under hösten förslag till Regionstyrelsen att tillsätta en utredning avseende personuppgiftsöverföringar till tredje land. Utredningen ska bland annat kartlägga de personuppgiftsöverföringar som sker till länder utanför EU/EES, vilket skydd dessa överföringar baseras på och eventuella brister i skyddet, möjligheterna att omförhandla eller bryta avtalen och konsekvenserna därav. Utredningens resultat föreslås presenteras under Q1 2021.

Parallellt med detta följer Dataskyddsombudet den utveckling som sker nationellt och på EU-nivå och uppdaterar organisationen när ny information finns tillgänglig.

Vid frågor kontakta Dataskyddsombudet, dataskyddsombud@regionvasterbotten.se.