2022-05-09 Förvaltningar och bolag i Göteborgs Stad

Dataskyddsenhetens uppdaterade rekommendationer om tredjelandsöverföringar efter Schrems II

Dataskyddsombudet ska enligt artikel 38.1 GDPR på ett korrekt sätt och i god tid delta i alla frågor som rör skyddet av personuppgifter. Dataskyddsombudet ska informera och ge råd, samt utfärda rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.[1]

Tidigare lämnade rekommendationer

Dataskyddsenheten skickade den 18 september 2020 ut skrivelsen ”Information till personuppgiftsansvariga styrelser och nämnder med anledning av EU-domstolens dom i mål C-311/18 (Schrems II-målet)” till samtliga förvaltningar och bolag i Göteborgs Stad. Denna skrivelse är en uppdatering, och utveckling, av de rekommendationer som tidigare lämnats av dataskyddsenheten i frågan.

Bakgrund

Syftet med dataskyddsförordningen (GDPR) är att säkerställa rätten till privatliv och rätten till skydd för personuppgifter, samt möjliggöra personuppgifternas fria flöde inom EU/EES. För att dessa rättigheter inte ska urholkas krävs tydliga regler för överföring av personuppgifter till länder som inte ingår i EU/EES. Tredjelandsöverföringar är inte tillåtna om den personuppgiftsansvarige eller personuppgiftsbiträdet inte kan säkerställa att GDPR efterlevs och att förutsättningarna i kapitel 5 GDPR är uppfyllda. Bestämmelserna i kapitel 5 ska tillämpas så att nivån på skyddet av fysiska personer som säkerställs genom förordningen inte undergrävs (artikel 44 GDPR).

I juli 2020 kom en dom från EU-domstolen (Schrems II-domen) som fick långtgående konsekvenser för överföringar av personuppgifter utanför EU/EES (till tredjeland). Domen sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt det som finns i EU/EES varför man antingen måste vidta extra skyddsåtgärder för att kunna föra över personuppgifter, eller avbryta behandlingen. Detta innebar också att det tidigare adekvansbeslutet (även kallat artikel 45-beslut) som fanns mellan EU och USA (Privacy Shield) ogiltigförklarades.

I Schrems II-domen kom domstolen fram till att amerikansk säkerhetslagstiftning (som möjliggör övervakningsprogram likt Prism och Upstream) medför att amerikanska myndigheter ges tillgång till personuppgifter för icke-amerikaner vid överföring av uppgifter från EU till USA. Domstolen bedömde att amerikansk lagstiftning som FISA 702 och EO 12333 (i anslutning till PPD 28) inte var begränsade till vad som kan anses

[1] *Riktlinjer om dataskyddsombud* (WP 243 rev.01), s. 20, senast granskade och antagna den 5 april 2017.

vara strikt nödvändigt och därmed inte heller uppfyller minimikraven för proportionalitet. Det konstaterades också att det saknas effektiva rättsmedel för icke-amerikaner.

Efter Schrems II

Efter domen, som nu är knappt två år gammal, har ett antal vägledningar och beslut från olika tillsynsmyndigheter kommit som på olika sätt tolkar domen. Här ska tilläggas att beslut från tillsynsmyndigheter inte är prejudicerande och har alltså inte samma status som domar från till exempel EU-domstolen. De visar dock hur experter på dataskyddsområdet resonerar och tolkar domen och hur bedömningar ser ut i enskilda frågor. Tillsynsmyndigheterna strävar också efter att göra enhetliga tolkningar i dataskyddsfrågor varför det är sannolikt att till exempel den svenska tillsynsmyndigheten skulle komma till samma eller i vart fall liknande slutsatser som andra tillsynsmyndigheter. Vad gäller vägledningar är det särskilt de från EDPB (Europeiska dataskyddsstyrelsen) som är relevanta.

Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter.

Denna vägledning innehåller rekommendationer om hur bedömningen av tredjeländer kan gå till och hjälp med att identifiera lämpliga kompletterande åtgärder.
Rekommendationen innehåller ett antal steg som kan följas. Metoden att följa dessa steg har fått namnet TIA (Transfer Impact Assessment) och är alltså ett sätt för de som vill överföra personuppgifter till tredjeland att kontrollera och säkra sin överföring.
Rekommendationen är landsneutral och tanken är att den ska vara möjlig att följa oavsett till vilket land utanför EU/EES som överföringen ska ske.

Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder

Som framgår ovan består rekommendation 01/2020 av ett antal steg som kan följas för att kontrollera en överföring till tredje land. Det tredje steget innebär en bedömning av ”om det finns något i rättsläget och/eller gällande praxis i tredjelandet som kan påverka effektiviteten hos de lämpliga skyddsåtgärderna i de överföringsverktyg som du använder i samband med din överföring”. För att få hjälp i denna komplicerade bedömning har EDPB tagit fram rekommendationer 02/2020 som alltså anger vad i det mottagande landets lagstiftning/praxis som man behöver vara vaksam på och kontrollera särskilt.

Beslut och uttalanden från tillsynsmyndigheter (ett urval)

Österrikiska tillsynsmyndigheten (DSB), januari 2022[2]: Efter klagomål från en enskild beslutade DSB att en webbplatsoperatör brutit mot artikel 44 GDPR genom att använda Google Analytics och därmed överfört personuppgifter utan att säkerställa en adekvat skyddsnivå. Vid överföringen lutade sig Google mot överföringsverktyget ”standardavtalsklausuler” enligt artikel 46 GDPR samt kompletterande åtgärd i form av kryptering (encryption at rest). Denna ansågs dock inte tillräcklig varför överföringen stod i strid med GDPR.

[2] https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal

Franska tillsynsmyndigheten (CNIL), februari 2022[3]: Bedömde att överföringen av personuppgifter till USA via Google Analytics av en webbplatsinnehavare skedde i strid med artikel 44 GDPR eftersom de kompletterande skyddsåtgärder som vidtagits inte var tillräckliga. CNIL beslutade att webbplatsinnehavaren av Google Analytics antingen behövde säkerställa följsamhet mot GDPR eller avbryta behandlingen.

Österrikiska tillsynsmyndigheten (DSB), maj 2022[4]: Beslut rörande Google Analytics med slutsatsen att överföringen av personuppgifter inte följde GDPR. I beslutet angav DSB uttryckligen att ett riskbaserat arbetssätt när det kommer till bedömningen av tredjelandsöverföringar inte är aktuellt. I GDPR framgår på flera ställen att ett riskbaserat arbetssätt ska tillämpas (bl.a. artikel 24, 25, 30 och 32 GDPR). Det står dock inte i kapitel 5 och de artiklar hänförliga till överföringar till tredjeland. Detta är ingen miss från lagstiftarens sida utan innebär att ett riskbaserat arbetssätt inte är tillämpbart när det kommer till bedömningen av tredjelandsöverföringar. Tilläggas kan också att EU-domstolen inte heller tillämpade detta arbetssätt i Schrems II-domen, eller ens nämner det som en möjlighet. Det är alltså inte möjligt att utifrån den aktuella risknivån göra en mer ”företagsvänlig” bedömning eller till exempel komma fram till att överföringen är följsam mot GDPR om bara icke-känsliga personuppgifter överförs.

Utöver de beslut som kommit från olika tillsynsmyndigheter har även vissa uttalanden gjorts. Till exempel har finska tillsynsmyndigheten Dataombudsmannen uttalat att användningen av Google Analytics inte är förenlig med dataskyddsförordningen pga. överföringen av personuppgifter till USA. Liknande uttalanden har gjorts av tillsynsmyndigheter i Norge och Lichtenstein.

Dataskyddsenhetens bedömning

Schrems II-domen har medfört ett stort antal vägledningar och tolkningar som på många sätt har klargjort hur tredjelandsöverföringar ska bedömas och vad ”likvärdig skyddsnivå” faktiskt innebär. Detta är vägledningar och rekommendationer som är tillämpliga på alla överföringar till länder utanför EU/EES och som framåt kommer att vara till stor hjälp. Det kan dock konstateras att överföringar av personuppgifter till USA fortsatt är mycket problematiska på grund av det rådande rättsläget i landet.

Bedömning av rättsläget i USA

I Schrems II-domen gjorde EU-domstolen en genomlysning av amerikansk lagstiftning och praxis och kom fram till att skyddet för personuppgifter för icke-amerikaner är otillräckligt. Denna lagstiftning och praxis har hittills inte ändrats eller förbättrats så att skyddet för personuppgifter har stärkts. Läget är (för närvarande) alltså likadant som det var vid tiden för Schrems II-domen. Eftersom inga ändringar har skett finns det ingen anledning för de som vill överföra personuppgifter till USA att göra en egen analys av det amerikanska rättsläget. Denna bedömning har redan gjorts av EU-domstolen i Schrems II-domen.

Ej möjligt att tillämpa ett riskbaserat arbetssätt

Dataskyddsenheten bedömning är, i likhet med österrikiska tillsynsmyndighetens, att det inte heller är aktuellt att göra en riskbedömning i de fall där en överföring av

[3] https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply
[4] https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf

personuppgifter till USA sker. Även om överföringen inte innefattar känsliga personuppgifter sker det en överföring av personuppgifter, som alltså måste följa GDPR.

Det är i dataskyddsenhetens mening inte heller aktuellt att göra en riskbedömning i de fall då det kan finnas en indirekt överföring. Med indirekt överföring menas de fall då till exempel lagring av personuppgifterna sker inom EU/EES men leverantören är amerikansk eller amerikanskägd och därmed omfattas av amerikansk extraterritoriell lagstiftning (som till exempel Cloud Act och FISA 702). Om detta stämmer in på leverantören kan de komma att behöva lämna ut uppgifter till amerikanska myndigheter. Om utlämning skulle ske medför det en överföring av personuppgifter till USA. För denna typ av leverantörer föreligger alltså alltid en risk för tredjelandsöverföring, även om uppgifterna enbart lagras inom EU/EES och om avsikten enbart är att personuppgifterna ska behandlas inom detta område. Dataskyddsenhetens bedömning är att det i dessa fall inte är möjligt att göra en korrekt uppskattning av **risken för att en överföring ska ske** eftersom leverantörer enligt tillämplig lag i flera fall är förhindrade från att berätta om vad som lämnas ut. Det går därför inte för en personuppgiftsansvarig att veta vilka uppgifter som samlas in, för vilket syfte och under vilken tid. Om risken inte kan bedömas vore det orimligt att förutsätta att risken för överföring är låg eller noll.

Tillräckliga kompletterande skyddsåtgärder

EU-domstolens bedömning i Schrems II-domen är relevant för alla leverantörer som passar in på definitionen ”electronic communications providers” och därmed träffas av FISA 702. För USA är avtalsmässiga och organisatoriska skyddsåtgärder inte tillräckliga. Det räcker alltså inte att till exempel avtala om att personuppgifter inte får lämnas ut till amerikanska myndigheter eftersom amerikanska myndigheter inte är bundna av avtalet. Tekniska skyddsåtgärder är enbart effektiva om de i praktiken förhindrar åtkomst av amerikanska myndigheter. Det innebär till exempel att kryptering bara är en effektiv åtgärd så länge det kan garanteras att krypteringsnycklarna aldrig blir tillgängliga för amerikanska myndigheter. Om en amerikansk molntjänst skulle tillhandahålla en krypteringstjänst och krypteringsnycklarna kan nås av molntjänsten skulle amerikanska myndigheter även kunna få åtkomst till nycklarna och därmed göra krypteringsåtgärden ineffektiv och otillräcklig. Om kryptering används som åtgärd är det också viktigt att den håller en tillräckligt hög nivå och håller över tid.

Privacy Shield 2.0?

Den 25 mars 2022 annonserade USA och EU-kommissionen att de enats om en principöverenskommelse om ett nytt ramverk för överföringar av personuppgifter. USA har angett att de kommer vidta åtgärder för att stärka skyddet för privatlivet i samband med signalspaningsverksamhet. Understrykas ska dock att avtal ännu inte är på plats och när (om) det är formaliserat behöver det antas av båda parter.

Det ska också noteras att de två tidigare ramverken framtagna av EU-kommissionen, Safe Harbour och Privacy Shield, ogiltigförklarades av EU-domstolen i målen Schrems I och Schrems II. Det är alltså ännu oklart hur framtiden ser ut och om det nya ramverket är den långsiktiga och stabila lösning som krävs. Tills vidare rekommenderas därför förvaltningar och bolag fortsätta arbetet med att kartlägga och säkerställa sina behandlingar.

EDPB har uttalat sig om ramverket och trycker bland annat på att det ännu inte finns något avtal på plats. De som överför personuppgifter från EU/EES behöver därför fortsättningsvis följa EU-domstolens praxis och då särskilt domen i Schrems II-målet.

Rekommendationer och kommentarer

Om överföring av personuppgifter sker till ett land utanför EU/EES **som inte är USA** och mottagarlandet saknar adekvansbeslut rekommenderar dataskyddsenheten att förvaltningar och bolag i Göteborgs Stad följer stegen i EDPB:s rekommendationer 01/2020.

Om överföring sker till USA rekommenderar dataskyddsenheten att förvaltningar och bolag i Göteborgs Stad gör följande:

- Säkerställ att det finns ett tillämpligt överföringsverktyg, till exempel standardavtalsklausuler tillsammans med kompletterande tekniska skyddsåtgärder.
- Om tillräckliga skyddsåtgärder inte kan säkerställas, om det till exempel inte är möjligt att använda den tilltänkta tjänsten med personuppgifter i krypterad form, behöver det utredas om det personuppgiftsbiträde som överför personuppgifterna kan bytas. Eller om det är ett underbiträde som medför en problematisk överföring, möjligheten att byta underbiträde.
- Om det inte är möjligt att byta personuppgiftsbiträde/underbiträde är rekommendationen att personuppgiftsbehandlingen som innebär en otillåten tredjelandsöverföring avbryts.

Rekommendationer för avtal/licenser

I takt med att digitaliseringen ökar kommer frågan om privatliv, personuppgifter och integritet fortsatt att vara högaktuell. Förvaltningar och bolag behöver börja se långsiktigt på arbetet med att säkerställa skyddet för de registrerades fri- och rättigheter.

Dataskyddsenheten rekommenderar därför förvaltningar och bolag i Göteborgs Stad att **helt avstå** från att gå in i nya avtal där ovan beskriven tredjelandsproblematik föreligger eller riskerar att föreligga. Samma rekommendation gäller också för förlängning av befintliga avtal och/eller licenser.

Frågor?

Har ni frågor kring tredjelandsöverföring eller behöver råd och stöd är ni välkomna att kontakta dataskyddsenheten på dso@intraservice.goteborg.se.

Dataskyddsenheten

GÖTEBORGS STAD