Resebyråtjänster – frågor till ramavtalsleverantörerna gällande tredjelandsöverföringar

Namn på ramavtalsleverantör: American Express Global Business Travel/GBT Sweden AB (GBT)

Fråga 1A: I vilken utsträckning överför ni personuppgifter till tredje land utan adekvat skyddsnivå, exempelvis USA, vid utförande av tjänster enligt ramavtalet?

Svar: På American Express Global Business Travel (GBT) använder vi personlig information för att tillhandahålla resetjänster. Vi samlar också in information om resebokningar för att generera viktiga rapporter för reseansvariga hos våra kunder så att de kan spara pengar, och för riskhanteringsteam för att hitta resenärer i en nödsituation. Resetjänster innebär behandling av personlig information, inklusive namn, adresser, passnummer och resepreferenser.

Resor är i sig globala och kräver att data behandlas på en mängd potentiella platser. För att en resa ska kunna ske måste bokningsinformation delas med flygbolag, hotell och andra reseleverantörer runt om i världen. Dessa reseleverantörer kan vara vitt spridda företag som anställda kan boka resor med, och de kan vara placerade var som helst i världen.

När vi överför personlig information till reseleverantörer som flygbolag och hotell gör vi det på instruktion från individen. Reseleverantörerna är oberoende personuppgiftsansvariga och för dessa ad hoc-överföringar litar vi på undantaget i artikel 49 (1) c i EU: s GDPR.

Fråga 1B: I vilken utsträckning anlitar ni er av underleverantörer som överför personuppgifter till tredje land utan adekvat skyddsnivå, exempelvis USA, för er räkning?

Svar: Resor är i sig globala och kräver att data behandlas på en mängd potentiella platser. För att en resa ska kunna ske måste bokningsinformation delas med flygbolag, hotell och andra reseleverantörer runt om i världen. Dessa reseleverantörer kan vara vitt spridda företag som anställda kan boka resor med, och de kan vara placerade var som helst i världen.

När vi överför personlig information till reseleverantörer som flygbolag och hotell gör vi det på instruktion från individen. Reseleverantörerna är oberoende personuppgiftsansvariga och för dessa ad hoc-överföringar litar vi på undantaget i artikel 49 (1) c i EU: s GDPR.

Fråga 1C: Vilka kategorier av uppgifter (ex. identitetsuppgifter eller kontaktuppgifter) omfattas av överföringen?

Svar: På American Express Global Business Travel (GBT) använder vi personlig information för att tillhandahålla resetjänster. Vi samlar också in information om resebokningar för att generera viktiga rapporter för reseansvariga hos våra kunder så att de kan spara pengar, och för riskhanteringsteam för att hitta resenärer i en nödsituation. Resetjänster innebär behandling av personlig information, inklusive namn, adresser, passnummer och resepreferenser.

Fråga 2A: När personuppgifterna är överförda till USA – vilken amerikansk leverantör (ex. molntjänstleverantör) tillhandahåller den databas eller molntjänst (ex. GDS) i vilken personuppgifterna därefter behandlas/lagras?

Svar: Resor är i sig globala och kräver att data behandlas på en mängd potentiella platser. För att en resa ska kunna ske måste bokningsinformation delas med flygbolag, hotell och andra reseleverantörer runt om i världen. Dessa reseleverantörer kan vara vitt spridda företag som anställda kan boka resor med, och de kan vara placerade var som helst i världen.

Resor kräver också att bokningsinformation konsolideras i globala distributionssystem (GDS:er) som drivs av oberoende tredje parter som regleras enligt en EU-uppförandekod/Code of Conduct. GDS:erna är där flygbolagen lagrar sina flygmöjligheter och där resenärens bokning bibehålls.

GBT lagrar data i GBT:s datacenter. GBT har valt att samarbeta med AWS för att skapa en säker, dynamisk och flexibel molndatacenterinfrastrukturlösning (AWS IaaS-infrastruktur) i östra USA (Virginia) -regionen.

Fråga 2B: Träffas denna leverantör av den amerikanska övervaknings-lagstiftningen/FISA 702 i egenskap av en ”electronic communication service provider”?

Svar: Regeringar över hela världen har befogenhet att begära data för nationell säkerhet och underrättelsetjänst. Till skillnad från telekommunikationsleverantörer och internetföretag är vi i allmänhet inte mottagare av sådana rättsliga krav med tanke på vår bransch när det gäller företagsresor, och vi anser oss inte vara föremål för US Foreign Intelligence Surveillance Act ("FISA").

Fråga 3A: Förekommer överföringar av personuppgifter till tredje land utan adekvat skyddsnivå, exempelvis USA, även i fall då bokning inte gäller resa till det tredje landet?

Svar: Data lagras i GBT:s datacenter i USA. GBT är den enda affärsresebyrån som verkar under bindande företagsbestämmelser (Binding Corporate Rules, ”BCR”), ett strikt certifierings- och dataöverföringssystem som kräver att dataskyddsmyndigheter i hela Europa granskar och godkänner vårt program. BCR är erkända i andra jurisdiktioner runt om i världen. GBT fungerar som personuppgiftsansvarig enligt Europeiska unionens allmänna dataskyddsförordning (GDPR). GBT gör nödvändiga arrangemang med tillsynsmyndigheter när känsliga uppgifter behandlas och ordnar lagliga motiveringar för det komplexa nätet av internationella överföringar som resor kräver, inte bara med våra BCR utan också genom avtal med reseleverantörer, GDS-operatörer och partnerresebyråer som tillhandahåller lokal service runt om i världen.

Fråga 3B: När det gäller överföringar som avses i 3A – hur garanterar ni att bestämmelserna i kap. V i dataskyddsförordningen uppfylls vid överföring till sådant tredje land (dit bokningen inte gäller)? **Ange land och rättsligt stöd** (ex. bindande företagsbestämmelser/Binding Corporate Rules (BCR), standardavtalsklausuler eller undantag enligt artikel 49). Fler rader kan läggas till i tabellen vid behov.

Tredje land till vilket personuppgifter överförs	**Rättsligt stöd för överföringen**
USA	Bindande företagsbestämmelser/Binding Corporate Rules (BCR) för överföringar inom GBT och standardavtalsklausuler för tredjepartsöverföringar.

Fråga 3C: Har ni sett över möjligheterna att begränsa överföring av personuppgifter i sådana fall?

Svar: Ja. Vänligen se GBT:s dataskydds- och sekretessprinciper i vår globala sekretesspolicy på https://privacy.amexgbt.com/principles, där det tydligt framgår att vi använder den minsta möjliga mängden data som krävs.

Fråga 4: För det fall ni eller av er anlitade underleverantör använder BCR som stöd för överföring av personuppgifter till mottagare/underleverantör i tredje land utan adekvat skyddsnivå, exempelvis USA – vilka åtgärder har ni vidtagit för att säkerställa att dessa BCR i praktiken erbjuder ett skydd för personuppgifterna motsvarande det som ges genom dataskyddsförordningen? (Det kan ex. vara kontroll av att bestämmelserna är förenliga med den lagstiftning dit överföringen sker).

Svar: För att säkerställa lagliga överföringar inom vårt nätverk av leverantörer runt om i världen tillämpar vårt program flera kontroller. Vi valde att inte bli certifierade enligt Privacy Shield Scheme utan valde istället att använda EU-administrerade dataöverföringsmekanismer. Vi behandlar personlig information i enlighet med vårt omfattande globala sekretessprogram, inklusive styrning enligt våra bindande företagsbestämmelser/BCR. Personlig information förvaras säkert och överförs på lämpligt sätt till andra länder där vi arbetar efter behov

för att ge omedelbart lokal support. Oavsett var data överförs inom vår företagsfamilj förblir det enligt det EU-godkända BCR-programmets regler och förfaranden som säkerställer konsekvent integritets- och dataskyddskontroll över hela världen.

Vi är det enda resebyrån i världen med bindande företagsbestämmelser/BCR. Att ackrediteras med BCR föregås av en omfattande granskning av att våra sekretessprogram uppfyller EU:s dataskyddsregler, samt kräver godkännande av alla våra relevanta dataskyddsmyndigheter.

Vi övervakar noggrant våra oberoende, licensierade resebyråpartner och utbildar alla våra personuppgiftsbiträden i ett branschledande tredjepartsprogram för riskhantering. Programmet inkluderar tecknande av personuppgiftsbiträdesavtal med EU:s standardavtalsklausuler där det behövs för att säkerställa laglig överföring och konsekvent skydd.

Fråga 5: För det fall ni använder EU:s standardavtalsklausuler som stöd för överföring av personuppgifter till mottagare/underleverantör i tredje land utan adekvat skyddsnivå, exempelvis USA – vilka ytterligare åtgärder har ni vidtagit för att säkerställa att dessa standardavtalsklausuler uppfyller kraven enligt dataskyddsförordningen till följd av Schrems II-domen?

Svar: Vänligen se vårt svar på fråga 4

Fråga 6A: I vilken utsträckning skyddas personuppgifter som ni överför via datorkommunikation av tekniska åtgärder, ex. kryptering, när dessa överförs till tredje land?

Svar: Vi implementerar lämpliga tekniska och organisatoriska åtgärder som är utformade för att skydda personuppgifter från obehörig åtkomst och bearbetning, inklusive genom användning av kryptering under transitering (t.ex. HTTPS / SFTP via TLS, VPN (IPSEC / SSL) och SSH) och / eller, om det behövs, kryptering på innehållsnivå.

Fråga 6B: Vilken form av kryptering använder ni er av? Beskriv kortfattat processen vid krypteringen av de personuppgifter som ni behandlar.

Svar:

Beskrivning: Vi implementerar lämpliga tekniska och organisatoriska åtgärder som är utformade för att skydda personuppgifter från obehörig åtkomst och bearbetning, inklusive genom användning av kryptering under transitering (t.ex. HTTPS / SFTP via TLS, VPN (IPSEC / SSL) och SSH) och / eller, om det behövs, kryptering på innehållsnivå.