Resebyråtjänster – frågor till ramavtalsleverantörerna gällande tredjelandsöverföringar

Namn på ramavtalsleverantör: BCD Travel AB

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

Svar: BCD Travel är ett europeiskt bolag med huvudkontor i Nederländerna och vi är därigenom underkastade Europeisk reglering, inklusive GDPR och lokala dataskyddslagar. All överföring av personuppgifter sker i enlighet med GDPR och med stöd av EU:s standardavtalsklausuler.

BCD Travel bedriver en global affärsresebyråverksamhet. System och IT infrastruktur är utformade för att möta kundernas behov av effektiv reseservice. Våra datacenter finns inom EU/EES och USA. System och applikationer är optimerade på global basis vilket innebär att vi inom ramen för den löpande operativa verksamheten överför viss nödvändig data inklusive personuppgifter mellan EU/EES och USA i enlighet med gällande lagar.

Överföringar mellan globala BCD enheter sker på ett säkert sätt i vårt interna datanätverk med stöd av företagsinterna avtal baserat på EU standardavtalsklausuler. Överföring till externa tredjeparts leverantörer sker med stöd av EU standardavtalsklausuler.

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: I vår roll som oberoende personuppgiftsansvarig använder BCD Travel tredjepartsleverantörer för att utföra avtalade tjänster. Dessa tredjepartsleverantörer kan vara belägna utanför EU/EES eller använda underbiträden utanför EU/EES. BCD tredjepartsleverantörer tecknar skriftliga avtal, underkastas revision och kontroll och är skyldiga att följa alla tillämpliga dataskyddslagar, inklusive att överföring av personuppgifter till ett tredje land ska vara laglig. BCD Travel förblir ansvarig för sina underleverantörer.

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

Svar: De personuppgifter som överförs är sådana som krävs för resebokningar samt andra överenskomna tjänster. Uppgifterna är primärt namn och kontaktuppgifter men även andra kategorier av personuppgifter som är nödvändiga för att vi ska kunna tillhandahålla de tjänster som efterfrågas kan förekomma. Resenären kan även välja att inte tillhandahålla sådana uppgifter till BCD Travel och istället förmedla informationen direkt till den berörda tredjepartsleverantören.

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: Den huvudsakliga hantering av personuppgifter som överförs till USA sker primärt i vårt egna datacenter i Atlanta Georgia och sekundärt i ett datacenter i Lithia Springs (samlokalisering). För vissa specifika tjänster/lösningar sker hantering av personuppgifter av Amazon Web Services (AWS Virginia).

Hantering av resenärsprofiler sköts i vårt eget proprietära system som är baserat inom EU/EES.

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

Svar: BCD Travel är inte en leverantör av ”electronic communication service provider” såsom anges i Fisa 702.

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: Ja, eftersom våra interna processer stöds av system baserade på global IT infrastruktur som spänner över kontinenterna genom vårt interna datanätverk. För vidare detaljer se svar på fråga 1A och 1B.

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	EU Standardavtalsklausuler (SCC)

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

Svar: Ja, i enlighet med GDPR är det endast de personuppgifter som är nödvändiga för tjänstens utförande, t.ex. namn och kontaktuppgifter (mobil och epost), som hanteras och överförs. Kompletta resenärsprofiler och information gällande organisatorisk tillhörighet, kostnadsbärare etc. som används för administrative syften överförs inte.

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: Ej tillämpligt då BCD Travel inte förlitar sig på BCR vid överföring av personuppgifter.

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: BCD:s åtgärder efter Schrems II-beslutet omfattar översyn av tekniska, organisatoriska och administrativa åtgärder avseende överföring av personuppgifter utanför EU/EES. BCD Travel krypterar data, begränsar personuppgifter till vad som är nödvändigt för att tillhandahålla tjänsterna, implementerar rollbaserad tillgång till personuppgifter på behov av att veta och följer sin policy för arkivlagring. BCD fortsätter att granska och övervaka sina leverantörer och uppdatera sina databehandlingsavtal med leverantörer för att inkludera tillämplig reviderad SCC från juni 2021, prioritera leverantörer som kan komma åt personuppgifter om BCD Travels kunder, bekräfta skriftliga avtal med personuppgiftsbiträden kräver lämpliga säkerhetsåtgärder och regelbundet bedöma leverantörers integritets- och säkerhetsåtgärder.

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

Svar: BCD Travel krypterar data vid överföring och lagring. Krypteringsnycklar kontrolleras fullt ut av BCD travel.

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

Svar:

Kryptering vid överföring:
- Alla gränssnitt med webbläsare krypteras med TLS 1.2 och AES256
- Överföring i webbapplikationer krypteras med 2048 eller 4096 bitars RSA
- Även tillämpning av SHA2 certifikat förekommer
- Vid filöverföring används FTPS (stöd av TLS) eller SFTP (baserat på SSH)

Kryptering vid lagring:
- Hårdvarubaserad kryptering på media nivå vid back-up (AES 256)
- Arbetsstationer och bärbara datorer har krypterade diskar (AES 256)
- Applikationsservrar har tokensiserad och krypterad kreditkortsinformation (AES 256 och Liaison Token Manager)
- Mobila enheter (iOS och Android) är krypterade. För Android gäller: AES 256 och nyckelgenereringsfunktion baserat på PBKDF2 med HMAC-SHA1. För iOS gäller: 3DES.
- Applikationer som nyttjar Amazon Web Services (AWS) har krypterad data både i överföring och lagring (AES 256 och EBS encryption management), ingen kreditkortinformation lagras hos AWS

Observera att ovanstående standards revideras löpande.