Resebyråtjänster – frågor till ramavtalsleverantörerna gällande tredjelandsöverföringar

Namn på ramavtalsleverantör: Stureplans Affärsresebyrå AB

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

Svar: Inte alls.

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: Inte alls.

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

Svar: Inte aktuellt.

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: Inte aktuellt.

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

Svar: Inte aktuellt.

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: Nej.

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**

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

Svar: Vi har ingen överföring av personuppgifter till tredje land.

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: Våra underleverantörer överför ej personuppgifter till tredje land.

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: Ej aktuellt.

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 är PCI-certifierade, vilket bl.a. innebär att alla kreditkortsnummer och passnummer maskeras.

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

Svar: Vi är PCI-certifierade och maskerar all känslig information såsom kortuppgifter och passnummer.

Beskrivning: Vi har GDS Amadeus inklusive deras självbokningssystem cytric. För att säkra dessa data är anslutningen krypterad i båda riktningar och certifiering för PCI DSS 3.2 så TLS 1.2-krypteringsprotokoll är obligatoriskt. Se även beskrivning från Amadeus nedan:

Data Storage and Synchronization

Currently users may access the application in two different ways: Internet Browser & Interfaces such as SSO, Amadeus cytric T&E Webservices, Amadeus cytric T&E Companions, SAML2.0

To secure this data, the connection is encrypted in both directions and certification for PCI DSS 3.2 so TLS 1.2 encryption protocol mandatory.

· All data in transit and at rest is encrypted in the whole productive infrastructure.

· Data at rest is encrypted:

o AES256 for customer data stored in databases

o AS256 for database backups on disk / tape

· Data in transit is always encrypted with TLS1.2 using strong ciphers

· Bitlocker encryption is used for drives in mobile computers. Encryption mechanism for remote connections

· Encryption key management: HSM store encryption key. Key never leaves HSM. Access to key is managed by central key administration tool. Access to slots (for applications to encrypt data) provided by slot admins.

· Encryption technologies used: Secure Shell (SSH), Secure Sockets Layer (SSL), Internet Protocol Security (IPSEC)

· Back-up data encryption: AES256

Passwords to the web-based application are stored in the database and are encrypted whenever they are stored on IT equipment. The transmission of PANs (Primary Account Number) via email, SMS or any other end user technology. Only keys/certificates provided by trusted sources are accepted. Temporary passwords are unique, are not reused and comply with normal password guidelines.