Resebyråtjänster – frågor till ramavtalsleverantörerna gällande tredjelandsöverföringar

Namn på ramavtalsleverantör: Egencia Sweden AB

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

Svar: Som personuppgiftsansvarig är Egencia direkt ansvarig för att säkerställa efterlevnaden av EU:s regler för dataöverföring. För att uppnå efterlevnad har Egencia implementerat en koncernomfattande uppsättning "standardavtalsklausuler" (även kallade "modellklausuler"). Detta standardavtal om dataöverföring har godkänts av Europeiska kommissionen för att legitimera överföringar av personuppgifter från EU till länder utanför EU.

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: Expedia-gruppen utför noggrann granskning av våra leverantörers informationssäkerhetspraxis och kräver att leverantörer (inklusive de som behandlar kundpersonuppgifter för Egencias räkning) uppfyller omfattande säkerhetskrav, inklusive skyldigheter som kräver att leverantörer har på plats och upprätthåller lämpliga tekniska och organisatoriska åtgärder. Alla underleverantörer som har tillgång till vårt nätverk måste genomgå årlig, grundläggande säkerhetsutbildning.

Leverantörer får endast tillgång till resenärernas personuppgifter i syfte att tillhandahålla de specifika tjänster som anges i deras avtal med Egencia. Egencias leverantörsavtal beskriver exakt hur leverantören ska utföra dessa tjänster och införa standardbegränsningar för dataanvändning och datasäkerhetskrav för dessa leverantörer. Vidare tar Egencia kontraktsenligt ansvar för sina leverantörers serviceprestanda och dataskyddspraxis. Leverantörer är vanligtvis, men inte alltid, osynliga för Egencias resenärer. Nästan utan undantag har resenärer ingen oberoende relation med dessa leverantörer.

Egencia är personuppgiftsansvarig för resenärernas personuppgifter och som personuppgiftsansvarig är Egencia direkt ansvarig för att säkerställa efterlevnaden av dataskyddslagstiftningen (inklusive avtalsrelationer med personuppgiftsbiträden och deras underbiträden). Som referens finns Egencias underbiträdeslista på den här sidan: https://www.egencia.com/public/us/egencia-subprocessorlist?nabe=4740821671477248%3A1%2C5396162411233280%3A1%2C5560570001227776%3A1&nabr=10.

Observera att alla leverantörer som har tillgång till personuppgifter undersöks och måste gå igenom en säkerhetskonsekvensbedömning ("SIA"). Egencia har också robusta leverantörsbiträdesvillkor som krävs med alla leverantörer, vilket säkerställer flödet ner till någon av deras underbiträden.

Egencia kommer också att dela data med reseleverantörer (t.ex. flygbolag och hotell) vid resebokning, enligt personuppgiftsansvarig-till-personuppgiftsansvarig-basis.

Alla anställda och underentreprenörer som har tillgång till Egencias nätverk måste genomgå årlig grundläggande säkerhetsutbildning och måste läsa och underteckna Egencias policy för godkänd användning (som båda kräver att man accepterar Egencias standarder).

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

Svar: Egencia är ett globalt företag med huvudkontor i USA. Således behandlar Egencia resenärers personuppgifter utanför Europa, inklusive i USA, för olika ändamål inklusive rapporteringstjänster, redovisning och fakturering.

Egencia kommer endast att behandla information om dem som reser på uppdrag av sina företag, till exempel anställda, konsulter och arbetssökande ("resenärer"). Innan resenären använder Egencias webbplats kommer Egencia att kräva att de loggar in som användare med hjälp av ett användar-ID och lösenord. I allmänhet samlar Egencia in och lagrar all information som resenärerna tillhandahåller Egencia inklusive, utan begränsning, all personlig information om dem som de specifikt och frivilligt tillhandahåller eller ger oss på något annat sätt. Detta inkluderar information som kan identifiera dem, inklusive förnamn, efternamn, telefonnummer och e-postadress, passinformation och faktureringsinformation (till exempel kreditkortsnummer, kortinnehavarens namn och utgångsdatum). Vi kan också begära information om deras resepreferenser, inklusive måltidsförfrågningar, val av plats, information om medlemsprogram flyg/hotell/hyrbil och biljettalternativ. Andra anställda som deras Travel Manager, resebokare eller ansvarig chef kan ge Egencia ytterligare personlig information om resenärer som deras anställningsnummer.

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: Egencias servrar finns på Amazon Web Services Ireland Region och US West Region. Vi har också servrar i Amsterdam, Nederländerna och i Arizona, USA som endast drivs av den tekniska personalen i Egencia / Expedia på operatörsdatacenter som håller högsta nivå. Dessa datacenter ger säkerhet på hög nivå (säker byggnad, 24-timmars säkerhetsvakt, CCTV, brandskydd) och avbrotts-skydd (Tier II 2N +1, strömarkitektur, redundant internetanslutning). Egencias webbplats är ansluten till Amsterdam Internet Exchange (AMS-IX); ett av världens största Internetbörser och ansluten till ett globalt nätverk av Tier 1-operatörer. Varje server eller annan datacenterutrustning åtminstone fördubblas för att säkerställa att felet i ett system inte påverkar hela driftsfunktionen.

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

Svar: Ja. Egencia/Expedia Group är tekniskt sett en elektronisk kommunikationstjänst, eftersom den ger resenärer möjlighet att kommunicera med hotell och hyresfastigheter via Egencia / Expedia Groups samtalsplattform.

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: Se svar på fråga 1C ovan.

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.

Svar: Egencia är ett globalt företag med huvudkontor i USA. Således behandlar Egencia resenärers personuppgifter utanför Europa, inklusive i USA, för olika ändamål inklusive rapporteringstjänster, redovisning och fakturering.

Egencia tar datasekretess och säkerhet på största allvar och övervakar aktivt situationen. Som ni vet är rekommendationerna från EDPB och de uppdaterade standardavtalsklausulerna (SCCs) för närvarande i utkastform och är under samråd. Vi har granskat dokumenten noggrant och arbetar aktivt med att ta itu med rekommendationerna där så är lämpligt och genomförbart, men vi väntar på att de slutliga versionerna ska offentliggöras efter samrådet.

Egencia har historiskt förlitat sig på två mekanismer (i) Privacy Shield och (ii) Standard Contractual Clauses (SCC) för att reglera överföringen av data från EU till USA och våra kundavtal föreskriver båda mekanismerna. Trots den senaste ogiltigförklaringen av Privacy Shield-mekanismen kommer vi att fortsätta att följa principerna i Privacy Shield och har omcertifierat oavsett för att försäkra våra kunder om att ingenting har förändrats praktiskt, på det sätt vi skyddar personuppgifter. Vi har också interna SCCs på plats och kommer att fortsätta att förlita oss på dessa för överföringar ut ur EU. Kunder behöver därför inte ingå ytterligare SCCs med Egencia eftersom Egencia hanterar dataöverföringen inom Egencia-plattformen och våra koncerninterna SCCs täcker relevanta dataflöden.

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: N/A. Som nämns nedan i fråga 5 genomför Egencia lämpliga tekniska åtgärder med beaktande av bearbetningens natur och potentiella inverkan på de berörda registrerade. Dessa inkluderar:

- Enkryptering vid överföring av alla personuppgifter
- Enkryptering vid resten av alla känsliga personuppgifter

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: Som controller är Egencia direkt ansvarig för att säkerställa efterlevnaden av EU:s regler för dataexport. Se vårt svar på fråga 1B ovan.

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: Egencias kundavtal innehåller skyldigheter för Egencia att följa tillämplig dataskyddslagstiftning, vilket kräver att registeransvariga, till exempel Egencia, legitimerar dataöverföringar utanför EU.

SCCs är en giltig mekanism för överföring, under förutsättning att lämpliga riskbedömningar slutförs och kompletterande åtgärder införs för att skydda uppgifterna. Där resenärsdata överförs till USA från EU.

Egencia ska genomföra lämpliga tekniska, avtalsenliga och organisatoriska kompletterande åtgärder, med beaktande av behandlingens art och potentiella inverkan på de berörda registrerade. Dessa inkluderar:

- Kryptering under överföring av alla personuppgifter;
- Kryptering vid resten av alla känsliga personuppgifter;
- Ge insyn till våra kunder i förhållande till hur många förfrågningar om resenärsdata vi har fått från statliga organ i samband med övervakningsverksamhet, där det är lagligt tillåtet att göra det;
- Om Egencia får en amerikansk statlig begäran om tillgång till Resenärsdata ska Egencia bestrida ett sådant krav i den utsträckning som Egencia anser att en sådan efterfrågan strider mot Egencias skyldigheter enligt GDPR; och
- Se till att vi har dokumenterad intern politik som styr denna process.

Dessutom har Egencia inrättat och upprätthåller ett omfattande informationssäkerhetsprogram som inför många säkerhetskontroller. Egencias informationssystem skyddas av branschstandardbrandväggar och intrångsdetekteringssystem. Dessutom utförs regelbundna sårbarhetsskanningar, både automatiskt och manuellt av ett internt och dedikerat team av säkerhetsexperter. Egencia sårbarhets hanteringsprogram innehåller penetrations testning och program sårbarhets bedömningar för att säkerställa att säkerheten är korrekt konfigurerad och tillämpas i Egencia-miljön. All extern kommunikation och alla personuppgifter krypteras i överföringen. Detta säkerhetsåtagande har lett oss till att uppnå och upprätthålla starka säkerhetscertifieringar, inklusive PCI- DSS- och TÜV-certifieringar.

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

Svar: Egencia har olika krypterings- och datalagringsprinciper som är knutna till dataklassificering. Egencia klassificerar uppgifter i enlighet med EU-lagstiftningen i fyra kategorier (Mycket känslig, känslig, konfidentiell och offentlig information) enligt följande:

- **Mycket känslig information**: Den här uppsättningen data inkluderar konton för finansiering/betalning, inklusive kredit-/betalkortsnummer, autentiseringsdata, till exempel lösenord eller PIN-koder och personnummer. Dessa data måste alltid krypteras, både under transport och i vila, i interna Egencia-miljöer och i externa tredjepartsmiljöer.

- **Känslig information**: Denna uppsättning uppgifter innehåller information som kategoriseras som "känsliga uppgifter" enligt europeisk integritetslagstiftning (i dess direktiv 95/46/EG), såsom ras, religion, etnicitet, eller uppgifter om hälsa. Egencia behandlar i allmänhet inte denna typ av känsliga data, även om måltidspreferenser och tillgänglighetsförfrågningar kan avslöja sådana känsliga data. Denna data, när de överförs, med eller mellan externa miljöer från tredje part måste alltid krypteras. Känslig Egencia Information i vila i interna Egencia-miljöer och i externa tredjepartsmiljöer måste antingen krypteras eller lagras i en skyddad miljö.

- **Konfidentiell information**: Denna uppsättning uppgifter är mindre känslig, men som Expedia ändå är skyldigt att skydda på lämpligt sätt, till exempel kontaktuppgifter, IP-adress (beroende på omständigheter), köp- eller resehistorik, beteendeinformation, demografisk information (när den är kopplad till en individ och därigenom blir PII), födelsedatum eller ålder och medborgarskap. Denna data måste alltid krypteras under överföring med eller mellan externa miljöer från tredje part. Konfidentiell Egencia-information i vila i externa miljöer från tredje part måste krypteras eller säkras i en skyddad miljö.

- **Offentlig information**: Information som är tillgänglig i det offentliga rummet.

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

Svar: Vi använder TLS 1.2 för datakryptering under överföring och AES 256 för kryptering av inaktiva data.

Beskrivning: