POLITICA DI SICUREZZA DEI DATI DEI CLIENTI

230 Route des Dolines, 06560 VALBONNE
Tel: +33(0)9 72 10 05 90 - E-mail: solutions@my-travelplanet.com
www.my-travelplanet.com

TRAVEL PLANET France SAS con un capitale di 3.000.000 €
SIRET 384 221 925 00116 - APE 7911Z - IM62100003

Governance della Sicurezza dei Dati

1.1 Un Approccio Impegnato alla Sicurezza dei Dati dei Clienti

Travel Planet si impegna a prendere tutte le misure necessarie per garantire la sicurezza dei dati dei clienti.

Nel perseguimento dell'eccellenza nella cybersecurity, Travel Planet collabora con un fornitore di servizi specializzato, che ha svolto le seguenti attività nel 2017:

Audit di sicurezza del sistema informativo (ambiente di lavoro del personale, infrastruttura del datacenter, architettura applicativa)

Implementazione della conformità

Formazione dei responsabili dello sviluppo sulle pratiche di codifica sicura

1.1.1 Conformità al GDPR

La conformità al Regolamento Generale sulla Protezione dei Dati (GDPR) è stata formalizzata al momento della sua entrata in vigore.

1.2 Gestione della Sicurezza Basata sul Rischio

Per garantire un approccio alla sicurezza efficace e consapevole, Travel Planet conduce regolarmente audit di sicurezza del proprio sistema informativo.

Inoltre, le decisioni di investimento nella sicurezza sono guidate da un'analisi dei rischi basata sulle caratteristiche specifiche dell'attività di Travel Planet. Questa analisi dei rischi viene aggiornata ogni due anni.

Panoramica della gestione basata sul rischio:

Mappatura degli asset digitali

• Sistemi IT in cui i dati sono conservati o attraverso cui transitano

Valutazione delle potenziali minacce

• Minacce esterne e basate su internet

• Valutazione delle risorse disponibili

Analisi dei rischi

• Orientamento degli investimenti in sicurezza per affrontare i rischi più significativi

• Priorità sistematica alla sicurezza dei dati dei clienti

230 Route des Dolines, 06560 VALBONNE
Tel: +33(0)9 72 10 05 90 - E-mail: solutions@my-travelplanet.com
www.my-travelplanet.com
TRAVEL PLANET France SAS con un capitale di 3.000.000 €
SIRET 384 221 925 00116 - APE 7911Z - IM62100003

1.3 Linee Guida per il Personale di Travel Planet:

1.3.1 Restrizioni di Accesso ai Dati

Ogni dipendente di Travel Planet ricopre uno o più ruoli all'interno dell'azienda. A seconda del proprio ruolo, un dipendente ha accesso esclusivamente alle informazioni necessarie per svolgere le proprie mansioni. Inoltre, i membri del personale sono sensibilizzati sull'importanza di non rispondere a richieste interne o esterne di divulgazione di informazioni sui clienti.

1.3.2 Sicurezza degli Account e Accesso al Sistema Informativo

L'accesso al sistema informativo di Travel Planet è assegnato nominativamente agli individui, garantendo la tracciabilità degli accessi. Gli account dei dipendenti vengono disattivati in caso di uscita dall'azienda o di cambiamento di ruolo.

Nessun dato cliente è conservato sui computer dei dipendenti, che sono utilizzati esclusivamente come punti di accesso alle applicazioni web del sistema informativo.

La sicurezza degli account privilegiati (amministratori) è rinforzata tramite l'autenticazione a due fattori.

1.3.3 Formazione del Personale

La Travel Planet Academy è un programma di formazione interna che fornisce ai nuovi dipendenti una formazione specifica per il loro ruolo. Nell'ambito di questo programma è inclusa una formazione sulle migliori pratiche di protezione dei dati e sulla sensibilizzazione alla cyber igiene.

Conduciamo inoltre regolari campagne di comunicazione interna sui temi della protezione dei dati e della cyber igiene.

Conservazione e Utilizzo dei Dati Personali

2.1 Conservazione dei Dati Personali dei Clienti

Travel Planet non utilizza mai i dati dei clienti, direttamente o indirettamente, per scopi diversi dall'adempimento del proprio ruolo di Travel Management Company (TMC). Non acquistiamo né vendiamo mai dati dei clienti.

2.1.1 Dati Conservati

Travel Planet conserva solo i dati necessari per l'esecuzione del contratto con il cliente. Per quanto riguarda i dati personali, si tratta principalmente delle informazioni di identità essenziali per l'organizzazione dei viaggi. Non conserviamo alcuna informazione di pagamento.

2.1.2 Stampe

Gli itinerari di viaggio sono trattati interamente in formato digitale. Non effettuiamo stampe.

Solo l'elaborazione di richieste eccezionali può occasionalmente richiedere la creazione di un dossier cartaceo. In tali casi, i dossier sono conservati in armadi chiusi a chiave in uno dei siti sicuri di Travel Planet, con accesso regolato tramite badge.

Inoltre, i documenti cartacei vengono distrutti prima di essere smaltiti come rifiuti riciclabili.

2.1.3 Principi di Cybersecurity Relativi alla Conservazione Digitale dei Dati Personali

Per garantire la sicurezza dei dati personali all'interno del sistema informativo di Travel Planet, abbiamo implementato i principi architetturali descritti in questa sezione.

2.1.3.1 Vault dei Dati Personali

Tutti i dati personali dei nostri clienti sono conservati in un vault digitale dei dati personali.

Si tratta di un database sicuro che contiene dati personali. Definiamo dati personali tutte quelle informazioni che possono facilmente identificare un cliente, come i dati anagrafici (nome, cognome, ecc.) o i dati di contatto (numero di telefono, indirizzo postale, ecc.).

L'accesso a questo vault è strettamente limitato, e i dati sono conservati e criptati a livello applicativo (una query SQL al database restituirà informazioni criptate).

Per impostazione predefinita, le nostre applicazioni memorizzano ed elaborano dati anonimizzati collegati a un identificatore tecnico. Solo i processi che necessitano di accedere ai dati personali possono occasionalmente recuperarli utilizzando l'ID tecnico di correlazione per interrogare il vault.

2.1.3.2 Sicurezza nello Sviluppo delle Nostre Applicazioni Web

Tutte le transazioni con il client web avvengono all'interno di una sessione applicativa a tempo limitato. La sessione è gestita utilizzando un cookie standard autogenerato. Di conseguenza, tutte le transazioni client-server propagano l'identificatore di sessione.

Per proteggere il nostro client web da tentativi di hacking, eseguiamo sistematicamente controlli sui diritti di accesso su tutte le nostre API lato server utilizzando un token sicuro.

Qualsiasi situazione anomala (timeout, connessioni simultanee multiple, ecc.) durante una sessione comporta la chiusura della sessione stessa, obbligando l'utente a riconnettersi per ripristinare le condizioni normali. Inoltre, ci riserviamo il diritto di disattivare temporaneamente un account utente che presenti comportamenti anomali che possano far sospettare una compromissione.

2.2 Trattamento dei Dati Personali

Non effettuiamo alcun trattamento dei dati dei clienti al di fuori di quanto strettamente necessario per l'esecuzione del nostro servizio. Non vengono effettuate attività di arricchimento dei dati né altri utilizzi dei dati personali.

3.1.2 Sistema Avanzato di Filtraggio
 Utilizziamo una tecnologia di filtraggio che si applica a ciascuna macchina individualmente. In altre parole, per impostazione predefinita, anche due macchine (virtuali o fisiche) all'interno della stessa zona di rete non possono comunicare tra loro.
 Definiamo regole di filtraggio specializzate per ogni macchina in base al suo ruolo. È consentito solo il traffico di rete necessario al corretto funzionamento del sistema informativo. L'implementazione di questa tecnologia impone una disciplina rigorosa nella gestione del traffico di rete.

3.2 Manutenzione Operativa e Reporting sulla Sicurezza

3.2.1 Gestione dell'Obsolescenza e delle Patch
 I team di sviluppo e operazioni IT collaborano per mantenere l'integrità operativa e di sicurezza del sistema informativo. Questo processo si basa in particolare sul reporting di gestione dell'obsolescenza (inclusa la gestione delle patch) dei componenti del sistema (infrastruttura, sistema operativo, middleware e librerie applicative).

3.2.2 Accesso alle Console di Amministrazione
 L’ambiente di produzione è accessibile esclusivamente tramite console di amministrazione.
 Per massimizzarne la sicurezza, queste console sono effimere: vengono create quando un operatore deve eseguire un'attività di manutenzione e distrutte una volta completata l'attività. Di conseguenza, in condizioni normali, non esiste un accesso persistente alle "interfacce di amministrazione" delle macchine di produzione.

3.3 Rilevamento delle Intrusioni
 Abbiamo implementato una politica di logging per monitorare l'attività sul nostro sistema informativo.
 Ciò ci consente di raccogliere sia dati sulle prestazioni (tempi di risposta, ecc.) sia dati sulla sicurezza (log di accesso, ecc.).
 Questi log vengono elaborati utilizzando uno strumento di business intelligence.
 Alcuni di questi processi sono progettati per rilevare comportamenti anomali che possano indicare tentativi di intrusione o di esfiltrazione dei dati.
Quando viene rilevato un comportamento anomalo...