Travel Planet
Time to change
France

POLITIQUE DE SECURITE DES DONNEES CLIENTS

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

TRAVEL PLANET France SAS au capital de 3 000 000 €
SIRET 384 221 925 00116 – APE 7911Z – IM62100003

1. Gouvernance de la sécurité des données

1.1 Une démarche engagée en matière de sécurité des données clients

Travel Planet s'engage à faire le nécessaire pour sécuriser les données clients.
Dans un objectif d'excellence en matière de cybersécurité, Travel Planet se fait accompagner par un prestataire spécialisé qui a notamment effectué les missions suivantes sur l'année 2017 :

- Audit de sécurité du système d'information (environnement de travail du personnel, infrastructures datacenter, architecture applicative)
- Mise en conformité
- Formation des leads développeurs en sécurité des développements

1.1.1 Mise en conformité RGPD

La mise en conformité au Règlement Générale sur la Protection des Données a été régularisée lors de son entrée en vigueur.

1.2 Pilotage de la sécurité par les risques

Afin d'avoir une démarche de sécurité efficace et éclairée, Travel Planet réalise régulièrement des audits de sécurité sur son système d'information.
Par ailleurs le pilotage des investissements en sécurité est réalisé sur la base d'une analyse des risques inhérents aux spécificités du métier de Travel Planet. Cette analyse de risque est réévaluée tous les 2 ans.

Schéma de principe du pilotage par la connaissance des risques :

- Cartographie des actifs numériques
    - Systèmes informatiques dans lesquels ils sont stockés ou transitent

- Évaluation des menaces potentielles
    - Menaces externes et internet
    - Appréciation des moyens à disposition

- Analyse des risques
    - Pilotage des investissements sécurité pour parer aux risques les plus importants
    - Priorité systématique à la sécurité des données clients

1.3 Directives au personnel Travel Planet :

1.3.1 Restriction de l'accès aux données

Chaque membre du personnel Travel Planet possède un ou plusieurs rôles dans l'entreprise. En fonction de son rôle, un employé n'a accès qu'aux informations utiles à la réalisation de sa mission. Par ailleurs les membres du personnel sont sensibilisés à ne pas répondre aux éventuelles sollicitations, internes ou externes, de divulgation d'informations concernant les clients.

1.3.2 Sécurisation des comptes et accès au système d'information

Les accès au système d'information de Travel Planet sont nominatifs afin de permettre la traçabilité des accès. Les comptes des collaborateurs sont désactivés lors de leur départ ou lors d'un changement de rôle au sein de l'entreprise.
Aucune donnée client n'est stockée sur les postes de travail. Ceux-ci servent seulement de point d'accès aux applications web du système d'information.
La sécurité des comptes à privilèges (administrateurs) est renforcée par une authentification à 2 facteurs.

1.3.3 Formation du personnel

La Travel Planet Academy est un organisme de formation interne qui dispense une formation métier aux nouveaux employés. Nous avons intégré à ce parcours une formation aux bonnes pratiques en matière de protection des données, ainsi qu'une sensibilisation à la cyber-hygiène.
Nous menons également régulièrement des campagnes de communication interne sur ces thèmes de la protection des données et de la cyber-hygiène.

2. Stockage et utilisation des données personnelles

2.1 Stockage des données personnelles clients

Travel Planet n'exploite jamais directement ou indirectement les données clients à d'autres fins que l'exécution de sa seule mission de TMC. Nous n'achetons ou ne revendons jamais de données sur nos clients.

2.1.1 Données stockées

Travel Planet stocke exclusivement les données nécessaires à l'exécution du contrat conclue avec le client. En matière de données personnelles, cela concerne principalement les données d'identité indispensables à l'organisation des voyages. Nous ne stockons pas de moyen de paiement.

2.1.2 Impressions

Les dossiers de voyage sont intégralement traités numériquement. Nous n'imprimons pratiquement jamais de documents avec des données personnelles.

Seul le traitement des demandes exceptionnelles peut parfois passer par la composition d'un dossier papier. Dans ce cas, les dossiers sont stockés dans des armoires fermées sur l'un des sites Travel Planet, dont l'accès est sécurisé par badge.
Par ailleurs, les documents papiers sont détruits avant d'être évacués comme déchets recyclables.

2.1.3 Principes de cybersécurité liés au stockage numérique des données personnelles

Afin de garantir la sécurité des données personnelles contenues dans le système d'information Travel Planet, nous avons mis en place les principes d'architecture décrits dans ce paragraphe.

2.1.3.1 Coffre-fort des données personnelles

Toutes les données personnelles de nos clients sont stockées dans un coffre-fort numérique des données personnelles.
Il s'agit d'une base de données sécurisée qui contient les données personnelles. Nous appelons, ici, données personnelles toutes les données qui permettent aisément de retrouver l'identité réelle d'un client, tels que les éléments d'identité (nom, prénom…) ou encore les informations de contact (numéro de téléphone, adresse postale…). Les accès à ce coffre-fort sont limités au strict nécessaire et les données y sont stockées et chiffrées au niveau applicatif (une requête SQL dans la base remonte des informations chiffrées).
Par défaut nos applications stockent et traitent des données anonymes rattachées à un identifiant technique. Seuls les traitements qui exigent d'avoir accès aux données personnelles peuvent ponctuellement récupérer ces données en utilisant l'identifiant technique de corrélation pour appeler le coffre-fort.

2.1.3.2 Sécurité des développements de notre application web

Toutes les transactions avec le client web sont effectuées dans le cadre d'une session applicative à durée de vie limitée. La session est gérée classiquement sur base d'un cookie auto-généré. Dès lors, toutes les transactions client-serveur propageront l'identifiant de session.
Afin de nous protéger des tentatives de piratage de notre client web, nous effectuons des contrôles de droits d'accès systématiques sur toutes nos API côté serveur sur base d'un token sécurisé.
Toute situation anormale (time-out, connexions multiples simultanées…) sur une session entraine la destruction de celle-ci, demandant à l'utilisateur de se reconnecter pour retrouver une situation normale. Par ailleurs, nous nous réservons le droit de désactiver momentanément un compte utilisateur qui nous paraît avoir un comportement anormal pouvant présager qu'il serait piraté.

2.2 Traitements sur les données personnelles

Nous n'effectuons pas d'autres traitements sur les données clients que ceux strictement nécessaires à la réalisation de notre prestation. Aucun traitement d'enrichissement ou autres exploitations des données personnelles n'est effectué pour notre propre compte ou pour celui d'un tiers autre que le client lui-même.

2.3 Communication des données à des tiers

Nous ne communiquons les données qu'à des tiers identifiés et uniquement lorsque cela est directement nécessaire à la réalisation de notre prestation. Typiquement, nous communiquons les informations voyageurs (identité…) aux compagnies aériennes ou autres opérateurs de voyage lorsque nous réalisons une réservation pour le client.
En dehors du cas évoqué ci-dessus, nous ne vendons ou ne communiquons les données clients à personne.

3. Sécurité du système d'information

La sécurité des données client est directement liée à la sécurité du système d'information. Ce chapitre présente quelques principes qui illustrent la prise en compte de la cybersécurité dans la construction et la maintenance du SI Travel Planet.

3.1 Principes d'architecture du SI

3.1.1 Zones réseaux

Travel Planet a mis en place une segmentation réseau afin de limiter les possibilités de propagation en cas d'intrusion.
Le principe est que nous définissons plusieurs zones réseaux en fonction de leur niveau d'exposition (et donc inversement de sécurité). Il y a 3 zones d'hébergement classiques (High Risk Zone, Low Risk Zone et Secured Zone) ainsi qu'une zone dédiée à l'hébergement des composants d'administration.

Les usages typiques de ces zones sont les suivants :

- High Risk Zone
  - Héberge les composants directement exposés sur internet
- Low Risk Zone
  - Héberge les composants applicatifs qui ne sont pas exposés directement sur internet
  - Cette zone n'est accessible que depuis les locaux Travel Planet ou depuis la High Risk Zone avec un filtrage stricte des flux
- Secured Zone
  - Héberge les données
  - Cette zone n'est accessible que par filtrage stricte des flux. Par ailleurs, il n'est pas possible d'initier une connexion sortante depuis cette zone vers internet ou vers une autre zone de notre réseau datacenter. Cette mesure a pour vocation de compliquer l'exfiltration de données.

Par ailleurs nous maintenons un cloisonnement for entre les environnements (production, qualification…), le paterne de segmentation réseau décrit ci-dessus est donc répliqué par environnement.

3.1.2 Système de filtrage avancé

Nous utilisons une technologie de filtrage qui s'applique à chaque machine individuellement. Autrement dit, par défaut, même 2 machines (virtuelles ou physiques) d'une même zone réseau ne peuvent pas communiquer.
Nous définissons des règles de filtrage spécialisées pour chaque rôle de chaque machine. Ainsi seuls les flux nécessaires au bon fonctionnement du SI sont ouverts. La mise en place de cette technologie nous astreint à une discipline stricte de maîtrise de nos flux réseau.

3.2 Maintien en condition opérationnelle et reporting sécurité

3.2.1 Gestion de l'obsolescence et des patchs

Les équipes de développement et de production informatique travaillent ensemble au maintien en condition opérationnelle et de sécurité du SI. Ce processus est notamment basé sur un reporting de gestion de l'obsolescence (incluant le patch managment) des composants du SI (Infrastructures, OS, Middlewares et librairies applicatives).

3.2.2 Accès aux consoles d'administration

L'environnement de production ne peut être accédé que depuis des consoles d'administration. Afin de maximiser la sécurité de ces consoles, celles-ci sont éphémères. Elles sont créées lorsqu'un opérateur doit effectuer une opération de maintenance et détruites à la fin de cette opération. Ainsi en situation nominale, il n'existe aucun moyen d'accéder aux « interfaces d'administration » des machines de production.

3.3 Détection d'intrusion

Nous avons défini une politique de log pour surveiller l'activité sur notre système d'information. Cela nous permet de collecter des informations de performances (temps de réponse…) et de sécurité (accès…). Ces logs sont ensuite traités au moyen d'un outil de BI. Certains de ces traitements sont destinés à détecter des comportements atypiques pouvant correspondre à des tentatives d'intrusion ou d'exfiltration de données.
Lorsque des comportements anormaux sont détectés par ce billet, une investigation est réalisée par les équipes informatiques.