Par TravellerPad

Politique de confidentialité et RGPD

Ce document décrit comment TravellerPad, éditeur de la solution de gestion d'événements IWI.events, veille au respect du règlement RGPD et indique les mesures en place pour assurer la sécurité de vos données ainsi que des données personnelles de vos participants.

Qu'est-ce que le RGPD?

RGPD signifie «Règlement général sur la protection des données», un nouveau règlement au niveau européen qui entrera en vigueur le 25 mai 2018.

Les réglementations sont conçues pour harmoniser les lois sur la confidentialité des données à travers l'Europe, renforcer la protection des données personnelles des citoyens de l'UE et améliorer la manière dont les organisations traitent ces données. Il est très important de connaître les changements, car le non-respect peut entraîner de lourdes amendes pour les entreprises et les organisations.

En tant qu'organisateur d'événement, suis-je concerné?

Le changement le plus important est probablement la juridiction étendue du RGPD. À partir du 25 mai 2018, les règles en matière de protection des données s'appliqueront à toutes les entreprises traitant des données à caractère personnel de citoyens de l'UE, quel que soit leur lieu d'implantation.

Le RPGD s'appliquera également au traitement de données à caractère personnel par des citoyens de l'UE, dans le cadre duquel les activités concernent: l'offre de biens ou de services (gratuits ou payants) aux citoyens de l'UE, ainsi que la surveillance du comportement au sein de l'UE. Les entreprises non européennes qui traitent des données relatives aux citoyens de l'UE sont tenues de désigner un représentant dans l'UE.

Alors oui, tant que certains de vos participants sont citoyens de l'UE, vous êtes concernés et vos processus et outils doivent être conformes au RGPD.

Quels sont les risques de non-conformité?

Si votre entreprise ou votre organisation enfreint le RGPD, vous encourez une amende substantielle. Le maximum peut atteindre 4% de votre chiffre d'affaires global annuel ou 20

millions d'euros, selon le montant le plus élevé. Les amendes sont infligées pour des infractions telles que:

● consentement du client insuffisant pour traiter les données;

● violations du concept de confidentialité dès la conception;

● ne pas avoir vos dossiers en ordre;

● défaut d'avertir l'autorité compétente et les personnes concernées de la violation.

Quelles sont mes obligations, quelles sont les obligations de TravellerPad?

Le RGPD définit deux rôles dans le processus de traitement des données de vos participants: le contrôleur de données et le processeur de données.

Contrôleur de données (vous en tant qu'organisateur d'événement)

Contrôleur désigne la personne ou l'entreprise qui décide quelles informations sont collectées, à quelles fins et de quelle manière elles sont traitées. Selon le droit de l'UE, les obligations du responsable du traitement incluent, sans toutefois s'y limiter:

● fournir des informations claires à vos participants sur les données personnelles que vous collectez et dans quel but;

● obtenir le consentement clair du participant indiquant qu'il accepte de fournir ses données personnelles à cette fin précise ;

● donner au participant un moyen simple de demander que vous effaciez, interrompiez la dissémination ultérieure des données et demandiez éventuellement à des tiers d'interrompre le traitement des données, ainsi que de restituer ses données personnelles au participant dans un format lisible par l'homme (Excel par exemple).

TravellerPad a imposé, depuis mai 2018, que tous les sites Web d'inscription comportent un avis de non-responsabilité sur la page d'enregistrement, avec un texte normalisé couvrant ces 3 obligations. Nous vous conseillons vivement de vérifier ce texte avec votre service juridique interne ou le service juridique de votre client, afin de vous assurer qu'il est conforme aux politiques du pays ou de la société.

Les obligations du contrôleur incluent également:

● conserver et traiter uniquement les données absolument nécessaires à l'accomplissement de ses tâches (minimisation des données). De plus, ils doivent limiter l'accès des processeurs de données à ces données personnelles ;

● protéger les données personnelles contre la perte accidentelle, l'accès non autorisé ou le traitement illégal.

TravellerPad assure cette protection au niveau de la plate-forme (voir ci-dessous), mais la sécurité de votre boîte aux lettres, de votre ordinateur, de vos logiciels, etc. relève de votre responsabilité.

● établir des accords écrits avec les processeurs qui ont accès aux données de vos clients, les obligeant à agir uniquement selon vos instructions et à s'assurer qu'ils respectent toutes les exigences de protection des données ;

● informer les participants dans les 72 heures qui suivent la première découverte d'une violation de données ;

● s'assurer que tous les processeurs de données répondent aux exigences (voir ci-dessous).

Processeurs de données (TravellerPad et notre hébergeur, IONOS, et vos autres sous-traitants)

Processeur: toute personne ou entreprise traitant des données à caractère personnel pour le responsable du traitement, telle qu'une plate-forme d'enregistrement, une application événementielle, des analyses de données, des services d'hébergement ou de stockage, etc.

IMPORTANT: si vous exportez des données de la plate-forme TravellerPad, et donc du système de gestion d'événements IWI.events (par exemple sous forme de fichier Excel), vous êtes également un processeur de données. Les obligations des responsables du traitement des données s'appliquent également à vous et à tous vos sous-traitants avoir accès à ces données exportées (intervenants freelance affectés à la gestion des participants, sous-traitant de l'impression de badges, etc.).

Les exigences pour les processeurs incluent, mais ne se limitent pas à:

● traiter les données de manière loyale, licite et à des fins légitimes;

● mettre en œuvre toutes les mesures de sécurité appropriées pour protéger les données personnelles informer immédiatement le contrôleur de toute violation des données ;

● tenir des registres internes de toutes les activités de traitement de données ;

● appliquer la confidentialité dès la conception (Privacy by Design) : cela signifie l'inclusion de la protection des données dès la conception des systèmes, plutôt qu'un ajout. Plus spécifiquement, vous devez mettre en œuvre des mesures techniques et organisationnelles appropriées pour répondre aux exigences de la nouvelle réglementation et protéger les droits des personnes concernées.

TravellerPad a mis en place les mesures appropriées pour se conformer pleinement à ces exigences. (Voir ci-dessous)

Politique de sécurité des données de TravellerPad

Confidentialité dès la conception (Privacy by Design)

Depuis le début, le système de gestion d'événements IWI.events édité par TravellerPad a été construit sur le principe de confidentialité dès la conception.

● Chaque événement a sa propre plate-forme front (instance de notre solution), s'exécutant de manière totalement isolée sur nos serveurs dédiés hébergés chez IONOS et partageant la même base de données avec chaque instance de notre solution. Chaque événement utilise le même back-office et la même base de données, mais les données d'événement sont complètement séparées les unes des autres et possèdent leur propre clé de cryptage unique et appropriée.

● Chaque instance d'événement n'a aucun moyen de communiquer avec les autres instances d'événement, même sur le même serveur physique.

● Au sein d'une instance d'événement, les utilisateurs privilégiés (administrateurs chargés de l'inscription des participants) voient leur identité vérifiée avant attribution des privilèges.

● Dans une instance d'événement, un participant ne peut pas accéder aux données d'un autre participant, sauf dans le répertoire des participants, dans lequel vous pouvez choisir les champs à afficher. Par défaut, les e-mails, numéros de téléphone ou autres données sensibles ne sont pas incluses. Dans ce cas, ces données ne sont même pas téléchargées sur les ordinateurs des participants. Seuls les utilisateurs privilégiés nommés par vous (l'administrateur principal du client) peuvent y accéder.

- Parmi le personnel technique de TravellerPad, personne ne peut accéder au code source ou aux données de votre plate-forme événementielle sans l'approbation du CTO ou du CEO de TravellerPad.
- Sécurité des serveurs de pré-production et de production
- Les données sont hébergées exclusivement dans des serveurs dédiés IONOS en France, situés dans le centre de données principal IONOS à Niederlauterbach (France).
- Serveurs front (apache 2.4, php 7.x): CentOS Linux 7.2.1511, Plesk v12.5.30 avec CPHulk (protection contre la force brute) et un pare-feu intégré.
- Aucun de nos clients n'a accès à un accès administratif ou technique au serveur (pas d'accès FTP ou MariaDB, pas d'accès CPanel, pas d'accès shell, etc.).
- Mises à jour et correctifs entièrement automatisés pour Plesk et CentOS, avec résumé envoyé par e-mail au CSO, et vérification humaine tous les mois.
- Protection DDOS par IONOS
- Apache 2.4 / PHP 7
- Les accès administratifs au serveur sont filtrés IP au niveau du pare-feu (seule l'adresse IP de notre bureau est autorisée) et nécessitent l'accord technique de CTO ou du CEO de TravellerPad.
- La protection contre la force brute est appliquée sur IMAP, SMTP et tous les services.
- Journalisation: pare-feu de serveur, démon HTTP, CPHulk produisent un accès et des journaux d'erreurs analysés chaque semaine par rapport aux performances ou à la sécurité problèmes.
- Sauvegarde quotidienne des bases de données et des fichiers utilisateur, cryptée avec SHA-512, au serveur de stockage sécurisé
- Surveillance de la sauvegarde automatisée

Principes de sécurité du développement

Chaque contribution de code de nos développeurs est examinée par le CTO / CSO de TravellerPad, afin de vérifier les goulots d'étranglement liés aux performances et de s'assurer que chaque élément de code est conforme aux directives OWASP (https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Guide_Guide_Guide_Table_of_Contents), notamment:

Sécurité du transport:

- https obligatoire avec certificat entièrement fiable et HSTS
- les chiffrements faibles ou les protocoles ont été désactivés
- Qualité Qualys SSL Labs: A +

Sécurité du mot de passe et de l'authentification

- Mot de passe généré à l'aide de SHA-512, MD5 mt_rand (), stocké avec hachage à l'aide de salt et de bcrypt. Il n'y a pas de connexion automatique autorisée sur notre solution
- Chaque fichier multimédia est protégé par plusieurs jetons aléatoires avec un hachage de vérification très long: https://nameoftheventwebsite.com/trk/437-FDimZkGaIfmYdMDkimWTnkwsid1697a3505564affeec839987386ee0a41f0c08aeb2bb122b85d26e4d0a7fa4dde6ec5d4156451bfe7a71f3abc87ac28ecb051e2484b7c9dfa1ea917eb2921f69bda96f11b8c25
- L'unicité de chaque chaîne aléatoire est renforcée en stockant leur hachage sha256.
- Protection d'attaque par force brute basée sur 5 tentatives d'une IP, désactivant la possibilité de s'authentifier pour le compte
- L'accès administratif à l'instance est sécurisé à l'aide d'une authentification à un facteur
- Les cookies d'authentification et les cookies de session sont HttpOnly et Secure. Notre application stocke une représentation hachée de la valeur du cookie lorsqu'il est envoyé, puis compare la valeur du cookie reçu pour s'assurer qu'elles sont identiques.

Contenu mixte:

- Toutes les ressources sont chargées à partir du nom de domaine.
- Tous les fichiers multimédias sont chargés depuis un CDN hautement sécurisé avec un jeton unique et aléatoire avec un hachage de vérification très long.
- Forfait de requête intersite (XSRF ou CSRF): demande le déclenchement des données les modifications ne sont effectuées que par POST. Chaque demande POST est validée avec jeton CSRF. Si elle est manquante ou incorrecte, la demande est bloquée.
- Inclusion de script entre sites (XSSI): toutes les demandes JSON sont effectuées via POST seulement
- Clickjacking: en-tête X-Frame-Options: SAMEORIGIN envoyé sur chaque page

Contenu tiers: toutes les ressources sont servies à partir du serveur de site Web et du nom de domaine.

Validation d'entrée

- Injection SQL: toutes les requêtes contenant une entrée utilisateur utilisent des requêtes paramétrées
- XPath Injection: aucune utilisation de X-Path
- Injection LDAP: aucune utilisation des requêtes LDAP
- Injection de commande: pas d'utilisation de la ligne de commande dans le code php

Path Traversal: le redimensionnement et le recadrage automatiques des image valident le type MIME du fichier en cours de traitement et se limite au répertoire des images du contenu de l'utilisateur

XSS (Cross Site Scripting): les données collectées par l'utilisateur sont stockées et affichées à l'aide de fonction d'échappement appropriée

Integer Overflows : pour chaque entrée numérique, la longueur et le type sont validés

Entités externes XML: aucune ressource XML chargée depuis un système externe

Politique générale de sécurité du personnel

● Tous les employés travaillent à temps plein et ont signé un NDA spécifique couvrant toutes les données internes et clients.

● Aucun travailleur à temps partiel ou externe n'a accès aux instances des clients, sauf autorisation expresse du client.

● Seuls les employés requis sont autorisés à accéder aux données et ne sont pas autorisés à conserver une copie des données. Tous les employés ont accepté ce principe dans le cadre de leur NDA.

● Les employés ne sont pas autorisés à conserver une copie des données du client en dehors de l'instance du client. Toute copie provisoire (reçue par quelque biais que ce soit, y compris par courrier électronique, ou extraite de l'instance client doit être supprimée immédiatement après son utilisation). Toute extraction de données doit être effectuée par le client à l'aide de son accès administratif à la plate-forme. Nous n'acceptons pas l'extraction de données pour le compte de nos clients.

Politique de continuité d'activité

Chaque instance est sauvegardée après l'événement sur un centre de données sécurisé hors site. Les sauvegardes sont conservées pendant 30 jours jusqu'à la destruction des données.

Politique de conservation des données

Par défaut, nous conservons les données d'une instance d'événement pendant trente jours après le déploiement. Les données sont ensuite automatiquement effacées, y compris les sauvegardes.

Si nécessaire, vous pouvez nous demander d'augmenter ou de réduire cette période.

Des questions ?

Si vous avez besoin d'informations supplémentaires, vous pouvez nous contacter à info@travellerpad.com