MESURES DE SECURITE TECHNIQUES ET ORGANISATIONNELLES		
	MESURES TECHNIQUES	**STATUT AU 01 DECEMBRE 2018**
AUTHENTIFICATION DU PERSONNEL DE SOCIAL SHAKER AYANT ACCES AUX DONNEES	Identifiant unique par utilisateur (plateforme, accès au Google drive et aux serveurs)	**Mis en place**
	Mot de passe complexe. Les paramètres de connexion, choisis par le Salarié, doivent respecter les recommandations de la Commission Nationale de l'Informatique et des Libertés, et en particulier atteindre un niveau suffisant de complexité pour permettre une authentification forte : ils doivent contenir 8 caractères minimum, contenant 3 des 4 types de signe suivants : majuscules, minuscules, chiffres, caractères spéciaux.	**Mis en place**
	Stockage sécurisé des mots de passe : hachage, mots de passe stockés de manière cryptée	**Mis en place**
GESTION DES HABILITATIONS POUR LIMITER L'ACCES AUX SEULES DONNES DONT L'UTILISATEUR A BESOIN	Profils d'habilitation définis en séparant les tâches et les domaines de responsabilité : profils de différents types avec des catégories d'accès par module de notre plateforme (statistiques, gestion de team etc.)	**Mis en place**
	Suppression des permissions d'accès dès que les utilisateurs ne sont plus habilités	**Mis en place**
	Mise à jour automatique des habilitations dès que les utilisateurs intègrent ou quittent SOCIAL SHAKER ou changent de fonction	**Mis en place**
MISE EN PLACE D'UN SYSTÈME DE JOURNALISATION	Mise en place d'un système de "fichiers journaux" ou "logs" retraçant les activités des utilisateurs: les accès, les erreurs et alertes	**Mis en place**
	Système de journalisation qui zipe les informations au bout de 2 jours + suppressions manuelles en fonction des systèmes (différents serveurs de la plateforme, application, serveurs de développement) selon leur vitesse de remplissage	**Mis en place**
	log rotate pour chaque type de log	**En cours de mise en place**
	Seuls les membres de l'équipe informatique ont accès à ces journaux	**Mis en place**
	Examens périodiques des journaux pour détecter d'éventuelles anomalies et notifier toute violation dans les plus brefs délais	**Mis en place**
	Mécanisme de vérouillage automatique des sessions	**Mis en place**
	Installation d'un pare-feu pour limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail	**Attente de confirmation par le propriétaire des locaux**

SECURISATION DES POSTES DE TRAVAIL	Utilisation d'antivirus et mises jour régulières des antivirus	**En cours de mise en place**
	Configuration des logiciels pour que les mises à jour de sécurité se fassent automatiquement	**Mis en place**
	Stockage des données sur Google drive et serveurs dans le Cloud	**Mis en place**
	Disques durs externes réservés aux seuls membres de l'équipe technique	**Mis en place**
	Blocage d'applications téléchargées ne provenant pas de sources sûres	**Mis en place (par défaut sur Mac OS)**
	Suppression systématique de façon sécurisée des données présentes sur un poste avant sa	**Mis en place**
	Installation de mises à jour critiques des systèmes d'exploitation sans délai en programmant une vérification automatique et hebdomadaire, au sein de l'équipe technique	**Mis en place**
SECURISATION DES EQUIPEMENTS MOBILES	Mise en place de mécanismes maîtrisés de sauvegarde ou de synchronisation des ordinateurs portables pour éviter la perte des données stockées (tout est sur Google drive)	**Mis en place**
	Aucun document ne se trouve sur des supports mobiles, tout est dans le Cloud et les ordinateurs sont protégés par des mots de passe	**Mis en place**
	Verrouillage automatique des smartphones et mot de passe nécessaire pour le déverouillage	**Mis en place**
PROTECTION DU RESEAU INFORMATIQUE INTERNE	Gestion des reseaux WI-FI avec utilisation d'un chiffrement à l'état de l'art	**Mis en place**
	Distinction entre les réseaux ouverts aux invités et le réseau interne	**Mis en place**
	Pour les serveurs web utilisant obligatoirement HTTPS, les flux entrants sur cette machine ne sont autorisés que sur le port 443 et les autres ports sont bloqués	**Mis en place**
SECURISATION DES SERVEURS	Limitation de l'accès aux outils et interfaces d'administration aux seules personnes habilitées	**Mis en place**
	Installation automatique par Google Cloud des mises à jour critiques	**Mis en place**
	Mesures de sécurité contre les attaques d'injection	**Mis en place**
	Sauvegardes et back up des serveurs via Google	**Mis en place**
	Mise en œuvre du protocole TLS ou un protocole assurant le chiffrement et l'authentification au minimum pour tout échange de données sur Internet et vérifier sa mise en œuvre par des outils appropriés	**Mis en place**
SECURISATION DES SITES WEB	Mise en œuvre du protocole TLS sur tous les sites web en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre	**Mis en place**
	Utilisation de TLS obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques	**Mis en place**
	Limitation des ports de communication strictement nécessaires au bon fonctionnement des applications installées	**Mis en place**

SAUVEGARDE DES DONNEES	Sauvegardes fréquentes des données, notamment pour prévoir des sauvegardes incrémentales et des sauvegardes complètes à intervalles réguliers, via Google Cloud	**Mis en place**
	Stockage des données sur Google Cloud	**Mis en place**
	Protection des données sauvegardées autant que les données stockées sur Goole Cloud	**Mis en place**
	Sauvegardes des données transmises par réseau et chiffrement du canal de transmissions, gérés par Google Cloud	**Mis en place**
ARCHIVAGE DES DONNEES	Destruction de l'intégralité des données archivées, gérée par Goole Cloud	**Mis en place**
ENCADREMENT DE LA MAINTENANCE ET DESTRUCTION DES DONNEES	Mise en place d'une procédure de suppression autonome des profils par les utilisateurs de la plateforme SOCIAL SHAKER	**A compter de janvier 2019**
	Développement d'une procédure de suppression de tous les comptes utilisateurs inactifs depuis 3 ans et de toutes les données des clients et de leurs campagnes	**A compter de début 2019**
	Mise en place d'une suppression des données des prospects	**A venir**
	Développement d'une procédure de suppression de toutes les données des campagnes et des participants aux campagnes créées il y a plus de 24 mois	**A compter de fin juin 2018**
	Développement de la possibilité pour un client de supprimer ses campagnes quand il le souhaite, et mise en place dans le back office une visibilité immédiate sur la date à laquelle les données de leurs campagnes seront supprimées automatiquement au bout de 24 mois	**A compter de janvier 2019**
	Suppression de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin de contrat de location	**Mis en place**
SECURISATION DES ECHANGES AVEC LES AUTRES ORGANISMES	Chiffrement des données transmises via la messagerie électronique Google	**Mis en place**
	Utilisation de la dernière version du protocole HTTPS garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers	**Mis en place**
	Confidentialité des mots de passe et identification initiale avec un lien	**Mis en place**
PROTECTION DES LOCAUX	Installation des alarmes anti-intrusion et vérifier régulièrement leur fonctionnement	**Attente de confirmation par le propriétaire des locaux**
	Mise en place des détecteurs de fumées et des moyens de lutte contre les incendies et vérifier régulièrement leur fonctionnement	**Attente de confirmation par le propriétaire des locaux**
	Utilisation d'un badge individuel et nominatif pour accéder aux locaux	**Mis en place**
	Accompagnement des visiteurs par un membre de SOCIAL SHAKER	**Mis en place**
	Rangement des ordinateurs portables dans des placards fermés chaque soir ; les ordinateurs fixes n'ont pas de port pour des câbles de sécurité	**Mis en place**

ENCADREMENT DES DEVELOPPEMENTS INFORMATIQUES ET DE LA CREATION DES FORMULAIRES DE CREATION DE CAMPAGNES	Intégration de la protection de la vie privée, y compris ses exigences de sécurité des données, dès la conception de l'application ou du service : limitation de l'accès aux données, encapsule dans des objets, le transit se fait de manière sécurisée, les accès aux données ne se font que sur demande au sein de l'équipe et chez les clients.	**Mis en place**
	Environnement de test en local puis environnement de staging ou pré-prod	**Mis en place**
	Limitation des formulaires de création de campagne à 3 champs personnalisables maximum	**Mis en place**
	Ajout dans le formulaire côté back office client d'un champ pré-rédigé mais modifiable pour qu'il mette les informations (cf livret) liées à la confidentialité de manière directement visible, en plus de la politique de confidentialité et du reglement dans le footer de leurs jeux	**Mis en place**
	Ajout dans le formulaire côté back office client d'un picto d'alerte au niveau des cases d'opt ins avec un lien vers la liste des données sensibles et interdites/non recommandées à collecter.	**Mis en place**
	Modification dans le formulaire côté back office client de la pré-rédaction des 2 champs d'opt-in pour qu'ils soient conformes : montrer les infos minimum à mettre, tout en étant modifiables pour coller aux besoins de chaque client.	**Mis en place**
	Ajout dans notre formulaire d'inscription sur notre plateforme d'opt-ins conformes	**Mis en place**
INTEGRITE, CONFIDENTIALITE ET AUTHENTICITE DES DONNEES	Fonctions de hachage pour les mots de passe	**Mis en place**
	Pour le back office, la seule informationa acceptée est l'API, qui n'accepte comme source que nos apps	**Mis en place**
	Lors de l'insertion de la participation dans nos serveurs, le message contenant les données personnelles est haché	**Mis en place**
	Utilisation de l'algorithme AES ou AES-CBC pour le chiffrement symétrique	**Mis en place**
	Utiliser de clés de 128 bits	**Mis en place**
	Protection des clefs secrètes, avec mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr	**Mis en place**