SECURITE & PROTECTION DES DONNEES

MAJ 17 novembre 2021

Table des matières

Définitions préalables

Les termes débutant par une majuscule au sein du présent document, qu'ils soient utilisés au singulier ou au pluriel, auront la signification qui leur est donnée ci-après.

Solutions :	désigne les applications informatiques développées et mises en œuvre par la société emage-me. Ces applications se déclinent en une application mobile (disponible pour Android et iOS), et un portail web.
Utilisateur :	désigne toute personne bénéficiant d'un accès et d'un usage aux Solutions, sur son ordinateur ou son téléphone mobile.
Client :	désigne toute entité juridique sous contrat avec emage-me, et bénéficiant de ce fait pour son compte de licences d'utilisation des Solutions emage-me.
Utilisateur clé :	désigne un utilisateur placé sous la responsabilité du Client, et bénéficiant d'un accès au portail web emage-me, lui conférant un rôle d'administration de tout ou partie des Solutions emage-me pour le compte du Client.
Utilisateur :	désigne un utilisateur ayant accès à la Solution application mobile emage-me.
Parcours :	désigne une expérience utilisateur et un ensemble de contenus digitaux personnalisés par le Client sur une Solution emage-me, auxquels un Utilisateur à accès via une action explicite de commencer cette expérience utilisateur dédiée au Client.

CR

1. Principes de la confidentialité des données

Principe général de propriété et visibilité des données

Les Solutions emage-me sont conçues pour limiter aux maximum l'accès aux données, et garantir ainsi la confidentialité, la profondeur et la sincérité des tous les échanges sur les Solutions.

Par principe, toutes les données saisies par l'Utilisateur sont la propriété de l'Utilisateur :

- L'Utilisateur décide si ces informations peuvent être transmises tout ou partie aux Clients, dans le cadre des Parcours dans lesquels l'Utilisateur s'inscrit volontairement et consciemment.

- L'Utilisateur peut en conséquence choisir à tout moment de ne plus partager ses données avec les Clients.

emage-me limite l'utilisation des données Utilisateurs aux cas suivants, clairement mentionnés aux Utilisateurs lors de leur inscription nominative sur les Solutions :

- Permettre un affichage de contenu adapté à l'utilisateur, en fonction de son profil

- Aider l'Utilisateur dans ses démarches volontaires auprès des Clients

- Réaliser des statistiques globales et anonymisées sur les usages pour optimiser les Solutions

- Administrer les Solution (en particulier concernant la modération des contenus)

Les Clients peuvent renseigner sur la Solution portail web des données supplémentaires, enrichissant les données Utilisateur qui leur sont partagés. Chaque Client est propriétaire des données qu'il saisit.

emage-me limite l'utilisation des données du Client aux usages du Client :

- Permettre la configuration des Parcours du Client sur les Solutions

- Assurer le support des Utilisateurs Clés

CR

Acteurs ayant accès aux données

L'accès aux données est en conséquence structuré comme suit :

- **Accès par défaut aux données Utilisateurs** : Par défaut, seul l'utilisateur a accès à ses données saisies sur les Solutions, ainsi que emage-me (cf. détail dans le paragraphe 2).
- **Ouverture d'un accès au Client** : l'Utilisateur peut choisir de s'inscrire à un parcours Client, et accepte alors de partager tout ou partie de ses données au Client. L'Utilisateur personnalise le niveau d'accès à ses données qu'il autorise au Client.
- **Accès aux données Client** : L'accès aux données du Client est limité aux personnes physiques qu'il autorise et qui sont sous sa responsabilité, et aux intervenants emage-me (cf. détail dans le paragraphe 2).

2. Formation & habilitation des intervenants

Formation du personnel

emage-me a met en place un processus de formation de tous ses effectifs pouvant être amené à avoir accès aux données des Utilisateurs et Clients.

Cette formation combine :

- Une formation initiale lors de l'intégration du collaborateur dans les effectifs : Temps dédié lors de la journée d'intégration du collaborateur.
- Une mise à niveau à minima annuelle : Destinée à l'ensemble des collaborateurs emage-me, elle permet d'actualiser les consignes dans le cadre de l'évolution des Solutions.

Lors de la formation initial, tout collaborateur emage-me :

- S'engage formellement à respecter la confidentialité desdites données, en signant une charte de confidentialité.
- Reçoit la formation nécessaire en matière de protection des données à caractère personnel

CR

Engagement formel du personnel

L'engagement formel du personnel sur la confidentialité des données porte notamment sur les points suivants, qui veut être complétés en fonction de besoins spécifiques :

- Ne pas utiliser les données auxquelles il peux accéder à des fins autres que celles prévues par ses attributions ;
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de ses fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- S'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- En cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Habilitation du personnel

emage-me limite l'accès aux données des Utilisateurs et Clients à un nombre très restreint d'intervenants.

Dans ce cadre, un tableau des accès est tenu à jour par la direction, et permet de tracer les personnes ayant accès aux données, ainsi que leur rôle et niveau d'habilitation.

Synthèse du tableau des habilitations au 17 novembre 2021 :

Fonction	Intervenant	Périmètre des accès
CTO	Brice ANTOINE	Global Clients & Utilisateurs
Responsable technique	Thibaud GRANIER	Global Clients & Utilisateurs
Développeur	Clément CHABRIER	Global Clients & Utilisateurs
Customer success	Anne-Clarisse LANTHEAUME	Clients uniquement
Customer success	Aurélie TREGARO	Clients uniquement

emage-me a mis en place les solutions technique de contrôle d'accès aux données pour bloquer tout accès par d'autres intervenants que ceux mentionnés ci-dessus.

CR

Limitation des accès sous-traitants

emage-me n'autorise pas ses sous-traitants à accéder aux données des Utilisateurs et Clients.

Lorsque nécessaire, emage-me met à disposition de ses sous-traitant un environnement de test, ne contenant pas de données Utilisateurs et Clients, pour leur permettre de réaliser leurs travaux.

L'accès à l'environnement de production contenant les données Utilisateurs et Clients est limité au personnel d'emage-me.

3. Processus de sécurisation des données

emage-me a déployé les processus suivants, dans le cadre de la sécurisation des données Utilisateurs et Clients.

Processus de conception orientée Privacy-by-Design

emage-me intègre la sécurité des données dès la phase de conception des Solution. Dans ce cadre, emage-me s'engage à prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de Privacy-by-Design et de protection des données par défaut.

Processus de gestion des demandes RGPD

emage-me a déployé les processus liés à l'exécution de ses obligations légales en lien avec le respect des droits des Utilisateurs et Clients, à savoir les droits :

- **à l'information** : information des Utilisateurs lors de la collecte de données, ou de l'inscription dans un process de collecte de données.
- **d'accès** : extraction et transmission aux Utilisateurs ou Clients des données qui lui sont confiées.
- **de rectification, d'effacement et d'opposition** : emage-me supporte les Utilisateurs et Clients dans le traitement de ces demandes, et s'assure de leur exécution.
- **à la limitation du traitement** : emage-me supporte les Utilisateurs et Clients dans le traitement de ces demandes.
- **à la portabilité des données** : emage-me fourni à la demande des Utilisateurs ou Clients les données dans un format structuré et lisible.

CR

Processus d'évaluation de la sécurité des données

emage-me met en place un processus d'évaluation régulière de la sécurité des données, sur une base annuelle. Cette évaluation peut être réalisée en interne, ou en externe.

Dans cadre, emage-me a désigné un chargé de projet, responsable de la protection des données, dont les coordonnées sont les suivantes :

Adresse électronique : christophe.roure@emage-me.com

- Coordonnées téléphoniques : +33(0)6 11 48 43 48
- Adresse postale : emage-me – 69 rue Gorge de Loup – Bat A – 69009 Lyon France

4. Solutions techniques de sécurisation

Infrastructure utilisée

Pour garantir un niveau de sécurité optimal, emage-me a opté pour l'utilisation d'une infrastructure gérée par GOOGLE.

Dans ce cadre, GOOGLE prend en charge pour le compte d'emage-me l'ensemble des services suivants :

- **Sécurité opérationnelle** :
  - Détection d'intrusion,
  - Détection des risques internes à emage-me,
  - Sécurisation des terminaux et identifiants des intervenants emage-me
- **Sécurité de l'accès en ligne** :
  - Garantie de disponibilité du service,
  - Protection contre les attaques (notamment DoS)
- **Sécurité du stockage de données** :
  - Chiffrement à froid de toutes les données stockées,
  - Suppression automatique des données obsolète

CR

- **Sécurité de l'authentification utilisateur** :
    - Fourniture du service d'authentification,
    - Double authentification requise pour les accès à la base de données
    - Protection contre les logins abusifs
- **Sécurité des services** :
    - Gestion des règles d'accès aux données des utilisateurs finaux,
    - Cryptage de bout en bout des échanges interservices,
    - Gestion des droits d'accès des échanges interservices
    - Contrôle de l'intégrité des services, et isolation des services
- **Sécurisation du matériel physique** :
    - Sécurisation de l'identité des machines physiques utilisées
    - Contrôle de la conception et de la provenance du matériel de stockage des données
    - Monitoring permanent de la sécurité de tous les éléments matériels de l'infrastructure emage-me.

Le détail de la solution de sécurité mise en place est disponible en suivant ce lien : https://cloud.google.com/security/infrastructure/design/

La conformité de cette infrastructure avec la réglementation RGPD est disponible en suivant ce lien : https://cloud.google.com/security/gdpr/

L'infrastructure mise en place pour emage-me est certifiée :

- ISO 27001 – ISO 27017 – ISO 27018 – AICPA SOC 11

Authentification des accès

Sur la base de l'infrastructure GOOGLE détaillée ci-dessus, emage-me gère un contrôle d'accès des différents usages comme suit :

- **Accès Utilisateurs** : L'accès se fait par vérification instantanée du numéro de téléphone, via SMS. emage-me n'a pas accès à la connexion en tant que cet Utilisateur.
- **Accès Client / Utilisateurs Clés** : L'accès se fait par email / mot de passe, avec application de règles strictes sur le niveau de complexité du mot de passe. emage-me n'a pas accès au mot de passe des Clients / Utilisateurs Clés.

CR

- **Accès emage-me** : L'accès emage-me au services GOOGLE assurant l'hébergement se fait par une double authentification nominative : Compte google puis vérification sur un autre terminal, incluant une détection d'accès inhabituel ou non autorisé (notamment en fonction de la location de la connexion).

Cryptage des données les plus sensibles

En complément du chiffrement à froid réalisé par GOOGLE sur l'intégralité des données, emage-me assure un chiffrement complémentaire à chaud sur les données les plus critiques.

Ceci concerne notamment le contenu des commentaires et feedbacks échangés via les Solutions.

De ce fait, les intervenants emage-me n'ont pas accès à ces données dans la base de données.

L'ensemble des données sont également protégées contre tout accès pirate, car se révèlent illisibles avec chacun de ces niveaux de chiffrement.

Localisation des données

Les données des services emage-me sont exclusivement stockées en Europe.

Les données sont aujourd'hui dupliquées sur des serveurs à Francfort et à Londres.

Sauvegarde des données

Pour sécuriser la disponibilité des données des sauvegarde sont faites quotidiennement.

Ces sauvegardes sont chiffrées à froid.

Elles sont dupliquées sur les serveurs de Francfort et de Londres.

Pour éviter une faille de sécurité sur les sauvegardes, celles-ci sont également assurées sur l'infrastructure GOOGLE, à d'autres emplacements.

Les délais de rétention sont les suivants :

- 1 semaine de rétention sur les sauvegardes quotidiennes
- 1 mois de rétention sur les sauvegardes hebdomadaires

CR