

## Information de conformité en France.

Addendum Relatif à la Protection et à l'Hébergement des Données de Santé (HDS).

### Note juridique préalable

Le présent document constitue un avenant (Addendum) aux Conditions Générales d'Utilisation ou au Contrat de Licence du logiciel Défibeo (EULA). Il formalise les obligations des parties conformément à l'article 28 du RGPD et à l'article L.1111-8 du Code de la santé publique français relatif à l'hébergement de données de santé (HDS).

## 1. Désignation des Parties

Le Responsable de Traitement :

L'exploitant utilisateur de la solution Défibeo,  
Ci-après dénommé « **Le Client** ».

Le Sous-traitant :

La société éditrice du logiciel Défibeo (Deroesch),  
Ci-après dénommée « **L'Éditeur** ».

## 2. Objet de l'Addendum

Le présent Addendum a pour objet de définir les conditions dans lesquelles l'Éditeur s'engage à effectuer, pour le compte du Client, les opérations de traitement de données à caractère personnel nécessaires à la fourniture du logiciel de maintenance de défibrillateurs Défibeo.

Dans le cadre de l'exécution de ses prestations, l'Éditeur est amené à traiter des données à caractère personnel et certaines relatives à la santé des personnes physiques, soumettant de fait le traitement au cadre réglementaire de la certification HDS en vigueur en France.

## 3. Nature et Finalité du Traitement

Le logiciel Défibeo est une solution d'infogérance, FSM et GMAO pour les défibrillateurs. Les données sont traitées exclusivement pour les finalités suivantes :

- Assurer le suivi technique, réglementaire et préventif du parc de défibrillateurs du Client.
- Consigner l'historique des interventions et les rapports d'utilisation des appareils lors d'événements de réanimation (incluant potentiellement des données physiologiques de l'événement et l'identité des patients pris en charge).
- Garantir la traçabilité des actions de maintenance conformément aux obligations réglementaires des dispositifs médicaux (notamment selon les lois et directives).

## 4. Catégories de Données Traitées

Les catégories de données collectées et traitées incluent :

- Données d'identification des utilisateurs (techniciens, administrateurs) : Nom, prénom, adresse email, identifiant, journal des connexions.
- Données relatives aux dispositifs médicaux : Numéro de série, emplacement, état de la batterie et des électrodes, rapports d'auto-tests.
- Données de santé (liées à l'utilisation en situation réelle) : Date et heure du choc, données d'impédance, données d'identification du patient si renseignées par l'exploitant (Nom, prénom, âge).

## 5. Architecture d'Hébergement et Conformité HDS

Conformément aux dispositions de l'article L.1111-8 du Code de la santé publique, l'Éditeur s'engage à ce que l'infrastructure technique supportant le logiciel Défibeo soit certifiée HDS. L'architecture repose sur un dispositif hybride décrit ci-après :

### 5.1. Hébergement Principal (Cloud)

L'infrastructure applicative et les bases de données de production du logiciel Défibeo sont déployées sur la plateforme Google Cloud Platform (GCP) / Firebase.

- Localisation : Les serveurs et centres de données utilisés sont exclusivement situés dans la région Europe (France - Zone de Paris `europa-west9`).
- Certification du sous-traitant ultérieur : Google Cloud EMEA Limited dispose d'une certification HDS valide pour les activités 1, 2, 3 et 4 (Hébergement d'infrastructure physique et d'infrastructure virtuelle).

### 5.2. Redondance et Sauvegarde Rapprochée (Souveraineté Locale)

Afin de garantir la haute disponibilité, la continuité d'activité et la résilience des données face aux incidents majeurs, l'Éditeur opère un cluster de redondance et de sauvegarde externalisé.

- Localisation : Infrastructure propre et dédiée, hébergée sur le territoire français au sein d'un centre de données sécurisé situé à Anglet (64), France.
- Garanties de sécurité : Ce site secondaire réplique les données de manière chiffrée. L'Éditeur garantit que l'accès à ce site est restreint au personnel habilité et audité, maintenant un niveau de sécurité et de confidentialité rigoureusement équivalent aux exigences du référentiel HDS.

## 6. Obligations de l'Éditeur (Sous-traitant)

L'Éditeur s'engage à :

- Instructions : Traiter les données uniquement sur les instructions documentées du Client.
- Confidentialité : Veiller à ce que les personnes autorisées à traiter les données (personnel technique et support de Défibeo) s'engagent à respecter la confidentialité et reçoivent la formation nécessaire à la protection des données de santé.

- Sécurité : Mettre en œuvre des mesures techniques et organisationnelles appropriées (chiffrement des données au repos et en transit via protocole TLS/SSL, isolation des bases de données, authentification forte).
- Maintenance technique : Encadrer de manière stricte les accès à l'application par ses techniciens lors des opérations de télémaintenance (génération de logs d'audit non modifiables).
- Notification de violation : Notification au Client de toute violation de données dans un délai maximal de 48 heures après en avoir pris connaissance.

## **7. Obligations du Client (Responsable de Traitement)**

Le Client s'engage à collecter les données de santé de manière licite, à informer les personnes concernées (patients/utilisateurs) conformément au RGPD, et à configurer de manière sécurisée les droits d'accès de ses propres collaborateurs sur la plateforme Défibeo.

## **8. Durée et Sort des Données**

Le présent Addendum reste en vigueur pendant toute la durée du contrat de service Défibeo. À la fin du contrat, l'Éditeur s'engage, au choix du Client, à restituer l'intégralité des données au format standard (CSV ou JSON) ou à les détruire de manière sécurisée, y compris sur les serveurs de redondance situés à Anglet, et à en justifier par écrit.

## **9. Maintien en Condition Opérationnelle (MCO)**

Le présent Addendum s'applique exclusivement à la nouvelle version de Défibeo commercialisée à compter du 1er juin 2026. Conformément aux conditions de Maintien en Conditions Opérationnelles (MCO), les versions antérieures du logiciel ne sont pas éligibles à la migration vers l'infrastructure Google Cloud certifiée HDS.

(!) Si votre entreprise est établie en France, vous devrez migrer vers la nouvelle version pour être conforme.

Document publié le 5 Juillet 2026.

## (Rappel) Comment nous protégeons vos données.

Information gestion des données : Sécurité et Infrastructure de vos données.

Chez Défibeo, la sécurité de vos informations est notre priorité absolue. En tant que solution SaaS, nous avons mis en place une architecture de pointe garantissant une disponibilité totale et une protection rigoureuse de vos données.

### 1. Une infrastructure à triple redondance

Pour prévenir tout risque de perte ou d'interruption, vos données bénéficient d'un principe de triple redondance sur des serveurs hautement sécurisés :

- Production (Temps réel) : Vos bases de données sont gérées de manière sécurisée via les technologies Google Cloud SQL et Firebase, tandis que vos fichiers sont stockés sur Google Cloud Storage (exclusivement sur la zone France pour garantir la souveraineté des données sur le sol français).
- Haute Performance : Pour les traitements complexes, nous utilisons notre propre serveur propriétaire situé à Anglet, France (64). Ce centre de données bénéficie d'une architecture NVIDIA indépendante, offrant une puissance de calcul et une isolation thermique/électrique maximale. Par sécurité, la localisation exacte est non publique.
- Archivage (Sécurité long terme) : Les données dites « froides » (sauvegardes historiques) sont conservées sur Google Cloud Storage Archive, garantissant leur intégrité même après plusieurs années.

### 2. Conformité RGPD : Notre engagement

Défibeo est pleinement conforme au Règlement Général sur la Protection des Données (RGPD). Nous appliquons des principes stricts pour garantir le respect de votre vie privée :

- Dépersonnalisation des données : Comme indiqué dans nos outils statistiques, les informations sensibles liées aux victimes sont dépersonnalisées. Nous traitons l'usage, pas l'identité.
- Souveraineté Européenne : Vos données applicatives et vos fichiers sont hébergés en France (Paris et Pau). Aucune donnée n'est transférée hors de l'Union Européenne.
- Chiffrement : Toutes les communications entre votre navigateur et nos serveurs sont sécurisées par des protocoles de chiffrement de grade industriel, et vos données sont chiffrées au repos sur les infrastructures de Google.
- Droit d'accès et de contrôle : Vous restez propriétaire de vos données. Vous disposez à tout moment d'un droit d'accès, de rectification et d'exportation de vos informations.
- Contrôle des accès : Seul le personnel strictement habilité et lié par une clause de confidentialité peut accéder aux infrastructures de maintenance.

Le saviez-vous ? Grâce à notre architecture hybride (Google Cloud / Firebase + Serveur propriétaire à Anglet), Défibeo combine la flexibilité et la puissance des technologies de pointe de Google avec la proximité et la sécurité d'une infrastructure française indépendante.

Cette infrastructure garantit un **Plan de Reprise d'Activité (PRA)** optimal (infrastructure + données).

Les données sont conservées pendant toute la durée de notre accord.