RÉACTIS — Plateforme de Gestion de Crise

Documentation Conformité RGPD et Sécurité Réseau

Éditeur et propriétaire : IFclubs — représenté par Frédéric TAILLEZ

Contact : taillez.f@orange.fr

URL de la plateforme : https://crise.ifclubs.fr

Date du document : 25 juin 2026

Version : 1.0

1. Présentation de la plateforme Réactis

1.1 Nature et finalité

Réactis est une plateforme SaaS de gestion de crise conçue pour les établissements de santé. Elle permet d'ouvrir, piloter et clôturer une cellule de crise, de tenir une main courante numérique en temps réel, de notifier les parties prenantes par email, WhatsApp et Telegram, et de générer des rapports de retour d'expérience (RETEX) assistés par intelligence artificielle.

La plateforme est accessible via navigateur web sécurisé (HTTPS). Elle est hébergée sur un serveur dédié IONOS situé en France (UE).

1.2 Architecture technique

Stack technologique :

- Backend : Node.js / Express.js — port 6008
- Frontend : React 19 + Vite — interface web responsive
- Stockage des données : fichiers JSON chiffrés, aucune base de données relationnelle exposée
- Reverse proxy : Nginx avec TLS 1.2/1.3 (certificat Let's Encrypt)
- Notifications : SMTP OVH (TLS 465), WhatsApp Web API, Telegram Bot API
- IA : Groq (fournisseur par défaut) / Anthropic (secours) — désactivable par établissement client
- Sauvegardes : chiffrées AES-256-CBC, quotidiennes, rétention 30 jours

1.3 Données traitées

- Données des membres de la cellule de crise : prénom, nom, adresse email professionnelle
- Données de contacts d'urgence : nom de service, email institutionnel, téléphone (urgences, ARS, etc.)

- Main courante : messages opérationnels saisis par les membres pendant la crise
- Pièces jointes : documents opérationnels uploadés pendant la crise (PDF, images)
- Logs email : traçabilité des notifications envoyées (destinataires, objet, date)
- Données d'abonnement : email de facturation, référence de paiement

2. Conformité RGPD

2.1 Base légale des traitements (Article 6 RGPD)

Les traitements réalisés par Réactis reposent sur la base légale de l'intérêt légitime (Art. 6.1.f) pour la gestion opérationnelle des crises, et sur l'exécution d'un contrat (Art. 6.1.b) pour les données d'abonnement. Les données de santé nominatives des patients NE SONT PAS hébergées dans Réactis — la plateforme est un outil de coordination, pas de soins.

2.2 Rôles RGPD

Acteur	Rôle RGPD	Périmètre
L'établissement client	Responsable de traitement	Définit les finalités, habilite les membres de sa cellule de crise
IFclubs / Réactis	Sous-traitant (Art. 28)	Héberge et traite les données pour le compte du responsable de traitement
Groq (IA)	Sous-traitant ultérieur	Traitement des textes pour résumés et conseils IA (fournisseur par défaut)
Anthropic (IA)	Sous-traitant ultérieur	Traitement des textes pour résumés IA (fournisseur de secours)
OVH (SMTP)	Sous-traitant ultérieur	Acheminement des emails de notification

2.3 Contrat de sous-traitance (DPA — Art. 28)

Un Data Processing Agreement (DPA) conforme à l'article 28 du RGPD a été établi. Il est accessible à l'URL : https://crise.ifclubs.fr/dpa.html

Ce contrat précise :

- Les finalités pour lesquelles les données sont traitées
- Les mesures de sécurité techniques et organisationnelles mises en place
- La liste des sous-traitants ultérieurs (Groq, Anthropic, OVH, Meta)
- Les obligations en cas de violation de données
- Les conditions de suppression des données en fin de contrat

Le DPA doit être formellement accepté par l'établissement avant toute mise en production. La signature électronique est enregistrée dans la plateforme.

2.4 Registre des activités de traitement (Art. 30)

Le registre des traitements est accessible à l'URL : https://crise.ifclubs.fr/registre-traitements.html

Il recense les quatre activités de traitement principales :

- Gestion des cellules de crise (main courante, notifications, RETEX)
- Gestion des membres et contacts de la cellule
- Traçabilité des communications (log email)
- Administration et facturation (données d'abonnement)

2.5 Durée de conservation et politique de rétention

- Main courante et archives de crise : 5 ans.
- Logs email : conservation 12 mois, suppression automatique au-delà
- Données de compte : durée de l'abonnement + 3 ans (obligations comptables)
- Pièces jointes : supprimées à la clôture de la crise si demandé

Un export RGPD et une fonction de purge sont disponibles via le panneau administrateur.

2.6 Droits des personnes concernées

Conformément au RGPD, les personnes dont les données sont traitées (membres de la cellule de crise) disposent des droits suivants, exercés auprès du DPO :

- Droit d'accès (Art. 15) : export disponible sur demande
- Droit de rectification (Art. 16) : modification possible par l'administrateur
- Droit à l'effacement (Art. 17) : suppression du compte et des données associées
- Droit à la portabilité (Art. 20) : export JSON disponible
- Droit d'opposition (Art. 21) : applicable pour les traitements sur base d'intérêt légitime

Contact DPO : taillez.f@orange.fr

2.7 Gestion des violations de données (Art. 33-34)

En cas de violation de données à caractère personnel, l'éditeur (Réactis) s'engage à :

- Notifier le responsable de traitement dans les 72h suivant la prise de connaissance de l'incident
- Documenter la violation dans un registre des incidents
- Évaluer le risque pour les droits et libertés des personnes concernées

- Assister le responsable de traitement pour la notification à la CNIL si nécessaire

3. Sécurité réseau et conformité technique

3.1 Chiffrement des communications

- HTTPS obligatoire : TLS 1.2 minimum, TLS 1.3 préféré — certificat Let's Encrypt renouvelé automatiquement
- HSTS activé : force le HTTPS pour tous les navigateurs (Strict-Transport-Security)
- Toutes les API communiquent exclusivement via HTTPS (pas de HTTP en production)
- Les emails de notification transitent via SMTP OVH avec chiffrement TLS sur le port 465

3.2 Authentification et contrôle d'accès

- Authentification par mot de passe hashé (bcrypt, coût 10) — aucun mot de passe stocké en clair
- Header d'authentification sur toutes les routes API sensibles (x-admin-password)
- Rate limiting sur le login : 10 tentatives / 15 minutes (express-rate-limit) — prévention brute force
- Tokens de suivi individuels pour chaque membre de crise (lecture de la main courante sans compte)
- Isolation par tenant : chaque établissement accède uniquement à ses données
- Rappel RGPD obligatoire à chaque connexion : modal de sensibilisation affiché avant accès à la main courante, acquitté par l'utilisateur ("J'ai compris") — mesure organisationnelle de prévention contre la saisie de données de santé nominatives

3.3 Headers de sécurité HTTP

Les headers de sécurité suivants sont configurés sur le serveur Nginx et via helmet.js :

- X-Frame-Options: DENY — protection contre le clickjacking
- X-Content-Type-Options: nosniff — prévention du MIME sniffing
- Referrer-Policy: strict-origin-when-cross-origin
- Permissions-Policy: camera=(), microphone=(), geolocation=()
- Content-Security-Policy : configuré pour restreindre les sources de scripts
- X-XSS-Protection : 1; mode=block

3.4 Protection des données au repos

- Sauvegardes chiffrées AES-256-CBC quotidiennes — clé de déchiffrement séparée des données
- Fichiers de configuration sensibles (.env) en permissions 600 (lecture propriétaire uniquement)

- Dossier data/ en permissions 750 (non accessible via le web)
- Aucune donnée sensible dans les URLs ou les logs applicatifs

3.5 Validation et contrôle des entrées

- Validation du type MIME de tous les fichiers uploadés (PDF, images, documents Office uniquement)
- Limite de taille des fichiers : 20 Mo par upload
- Protection contre l'injection : utilisation de execFileSync (non-shell) pour les scripts Python
- Validation JSON stricte sur toutes les routes API
- Protection CORS : whitelist limitée à *.crise.ifclubs.fr

3.6 Disponibilité et continuité de service

- Monitoring automatique toutes les 5 minutes (monitor.sh) — redémarrage automatique si indisponible
- Alerte email en cas de panne prolongée
- Log d'audit append-only (audit.log) traçant toutes les ouvertures/fermetures/suppressions de crise
- Processus Node.js géré par systemd (redémarrage automatique au boot)

3.7 Gestion des sous-traitants ultérieurs

Sous-traitant	Localisation	Usage	Garanties RGPD
IONOS (hébergement)	serveur IONOS , France (UE)	Serveur dédié, stockage	Certifié ISO 27001, DPA disponible
OVH (SMTP)	France (UE)	Envoi emails notifications	Certifié HDS, DPA disponible
Groq (IA — défaut)	États-Unis — Clauses SCCs	Résumés IA, conseils tactiques, RETEX (fournisseur par défaut)	Privacy Policy Groq, données non conservées après appel API
Anthropic (IA — secours)	États-Unis — Clauses SCCs	Résumés IA de main courante (si Groq indisponible)	API Privacy Policy, données non conservées
Meta (WhatsApp)	États-Unis — Clauses SCCs	Notifications crise (best-effort)	CGU WhatsApp Business — voir note

Note WhatsApp : L'intégration WhatsApp utilise une librairie d'automatisation (whatsapp-web.js). Cette intégration est mentionnée dans les CGV comme fonctionnalité "best-effort" — elle peut être interrompue sans préavis par Meta. Une migration vers l'API officielle WhatsApp

Business Cloud est prévue. Les établissements souhaitant une conformité stricte peuvent désactiver cette fonctionnalité.

4. Cadre légal et contractuel

4.1 Documents légaux disponibles sur la plateforme

- Conditions Générales de Vente (CGV) : /cgv.html — 11 articles, prix, SLA, IP, résiliation
- Conditions Générales d'Utilisation (CGU) : /cgu.html — 11 articles, usages autorisés/interdits, IA
- Data Processing Agreement (DPA) : /dpa.html — Art. 28 RGPD, sous-traitants, sécurité, suppression
- Politique de confidentialité (RGPD) : /rgpd.html — droits des personnes, contact DPO
- Registre des traitements Art. 30 : /registre-traitements.html
- Accord commercial : acceptation tracée par horodatage dans la plateforme

4.2 Gestion des crises — Finalité des données traitées

La plateforme Réactis traite des données opérationnelles de gestion de crise. Ces données incluent :

- Des informations sur les ressources disponibles (lits, effectifs, matériel) — données non nominatives
- Des messages de coordination entre membres de la cellule — données nominatives des professionnels
- Des notifications à des contacts institutionnels (ARS, SAMU, partenaires) — coordonnées professionnelles

La plateforme NE traite PAS de données de santé nominatives des patients. Les mentions éventuelles de données opérationnelles (nombre de patients, taux d'occupation) sont agrégées et ne permettent pas l'identification individuelle d'un patient.

Afin de prévenir toute saisie involontaire de données nominatives, un message d'alerte est affiché à chaque connexion à la plateforme. Les utilisateurs reconnaissent explicitement, par un clic sur « J'ai compris », que la main courante est un outil de coordination et ne doit pas contenir d'informations médicales nominatives sur les patients. Cette acceptation est tracée côté client à chaque session.

4.3 Hébergement des données de santé (HDS)

La plateforme Réactis n'est pas un hébergeur de données de santé à caractère personnel (HDS) au sens de l'article L. 1111-8 du Code de la Santé Publique, dans la mesure où elle ne stocke pas de données de santé nominatives des

patients. Les données traitées sont des données organisationnelles et opérationnelles de crise.

Si l'établissement venait à inclure des données de santé nominatives dans la main courante, l'éditeur devrait être certifié HDS. Il est rappelé aux utilisateurs à la connexion que la main courante est un outil de coordination et ne doit pas contenir d'informations médicales nominatives sur les patients.

5. Réponse aux exigences HAS — Gestion de crise numérique

5.1 Référence aux critères HAS 3.1-09 (Continuité du SI)

Réactis constitue un élément de preuve pour les éléments évaluables suivants :

- Existence d'un outil de coordination de crise opérationnel et testé
- Traçabilité horodatée des actions et décisions pendant la crise (main courante)
- Capacité à notifier les parties prenantes internes et externes en temps réel
- Génération de rapports de RETEX documentant les leçons apprises

5.2 Exercices réalisés

La plateforme a été utilisée dans le cadre d'exercices et de crises réelles avec des établissements clients. Ces sessions permettent de valider l'opérationnalité du dispositif de gestion de crise numérique.

- Des exercices de simulation de crise (plans blancs, canicule, incidents techniques) ont été conduits avec succès
- Des crises réelles ont été pilotées avec traçabilité complète de la main courante et notification multi-canal
- Les rapports RETEX générés automatiquement ont été validés par les établissements participants

Ces exercices et crises réelles constituent des preuves de l'opérationnalité du dispositif. Les données spécifiques aux établissements restent strictement confidentielles.

5.3 Sécurité des données de crise

- Chaque crise est archivée avec son identifiant unique, sa date d'ouverture/fermeture, ses membres actifs
- Les archives sont conservées 5 ans et peuvent être exportées ou purgées à la demande
- Un log d'audit indépendant trace toutes les actions administratives (ouverture, fermeture, suppression)
- Les sauvegardes chiffrées garantissent la pérennité des archives de crise

6. Contacts et responsabilités

Éditeur et propriétaire de la plateforme :

IFclubs — représenté par Frédéric TAILLEZ

Contact : taillez.f@orange.fr

Responsable de traitement :

L'établissement client utilisateur de la plateforme (responsable de traitement au sens du RGPD Art. 4). Chaque établissement est identifié dans son contrat d'abonnement.

Délégué à la Protection des Données (DPO) :

Contact DPO Réactis (sous-traitant) : taillez.f@orange.fr Pour les demandes d'exercice de droits relatives aux données de crise, les personnes concernées doivent s'adresser au DPO de leur établissement (responsable de traitement).

Pour toute question RGPD ou demande d'exercice de droits, contacter le DPO par email.