

Conformité RGPD & Sécurité

Réactis — Plateforme de gestion de crise — IFClubs SAS

Version : 2.4 — 26 septembre 2026 (marques de lecture personnelles visibles de la seule personne, aucune donnée de crise en cache sur les appareils, intégrité du journal entre appareils ; demandes d'aide au régional sous alias, conformité et exercices remontés en compteurs, passerelle à annuaire minimal d'empreintes, contrôle des saisies, revue de sécurité du 26/09/2026) — version précédente 2.2 (triple surveillance : serveurs, alertes proactives, erreurs techniques ; contrôle automatique des adresses e-mail ; audit de sécurité des 23-24/09/2026 : protection du navigateur appliquée, comptes système isolés, Node.js 24, surveillance et support proactifs, sessions, emails en copie cachée) | **Éditeur :** IFClubs SAS, représentée par Frédéric Taillez | **Contact :** support@ifclubs.fr

Ce document rassemble en un seul endroit la présentation de la plateforme Réactis, sa conformité RGPD et ses mesures de sécurité réseau. Il est destiné aux établissements clients, à leurs DPO et à leurs RSSI dans le cadre de l'évaluation du service avant ou pendant un abonnement. Ce document remplace la version PDF (v1.0, 25 juin 2026) — désormais disponible sous forme de page web, imprimable proprement depuis le navigateur.

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 collaborative en temps réel, de notifier les parties prenantes par email, WhatsApp, Telegram, Teams et SMS (niveau régional), 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 **VPS mutualisé IONOS** situé en France (UE).

1.2 Architecture technique

COUCHE	TECHNOLOGIE
Backend	Node.js 24 LTS / Express.js — un processus dédié par établissement (tenant), exécuté sous un compte système propre et non privilégié
Frontend	HTML / CSS / JavaScript, servi statiquement par Express — pas de framework compilé côté client
Stockage des données	Fichiers JSON sur disque, un jeu de fichiers distinct par établissement — aucune base de données relationnelle exposée
Reverse proxy	Nginx — TLS 1.2/1.3, certificat Let's Encrypt renouvelé automatiquement
Notifications	SMTP configuré par l'établissement client, WhatsApp Business, Telegram Bot API, Microsoft Teams (webhook), SMS (niveau régional, optionnel)
Intelligence artificielle	Mistral AI (fournisseur par défaut, France/UE) — Groq, Anthropic Claude et Azure OpenAI disponibles en alternative, interchangeables par le client lui-même depuis son panneau admin. Aucun basculement automatique entre fournisseurs : le tenant reste strictement sur celui qu'il a configuré.
Sauvegardes	Archives chiffrées AES-256, quotidiennes, rétention 30 jours glissants, clé dédiée par établissement

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)
- Numéros de téléphone mobile (destinataires SMS, niveau régional uniquement — canal désactivé par défaut)
- Données d'abonnement : email de facturation, référence de paiement
- Données techniques de fonctionnement (depuis le 25/09/2026) : date de dernière connexion de chaque membre (bilan de préparation de l'établissement), journal des envois d'alerte en échec (canal, motif technique, adresses masquées), erreurs techniques rencontrées dans l'application (message technique, fichier et page concernés — jamais les données saisies), empreintes des jetons de session

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 SAS / Réactis	Sous-traitant (Art. 28)	Héberge et traite les données pour le compte du responsable de traitement
Mistral AI	Sous-traitant ultérieur	Traitement des textes pour synthèse et conseils IA (fournisseur par défaut)
Groq / Anthropic / Azure OpenAI	Sous-traitant ultérieur	Traitement IA — optionnel, activable par le client à la place de Mistral AI
Anthropic	Sous-traitant ultérieur	Synthèses automatiques des niveaux régional et national : utilisé automatiquement pour les synthèses des niveaux régional et national depuis le 27/09/2026, sur des éléments déjà filtrés et pseudonymisés (aucune donnée patient ni coordonnée du personnel)
Scaleway SAS	Sous-traitant ultérieur	Alertes SMS niveau régional — optionnel, désactivé par défaut
Fournisseur SMTP	Sous-traitant ultérieur	Acheminement des emails de notification — configuré et choisi par l'établissement

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

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

Ce contrat précise les finalités de traitement, les mesures de sécurité techniques et organisationnelles, la liste des sous-traitants ultérieurs, les obligations en cas de violation de données, et les conditions de suppression des données en fin de contrat. Il doit être formellement accepté par l'établissement avant toute mise en production ; l'acceptation est enregistrée dans la plateforme.

2.4 Registre des activités de traitement (Art. 30)

Accessible à l'URL : crise.ifclubs.fr/registre-traitements.html. Il recense les activités principales : gestion des cellules de crise (main courante, notifications, RETEX), gestion des membres et contacts de la cellule, traçabilité des communications, administration et facturation.

2.5 Durée de conservation et politique de rétention

- **Main courante et archives de crise** : 5 ans par défaut après la date de clôture, configurable par l'établissement
- **RETEX (retours d'expérience)** : non soumis à la purge automatique — conservés indéfiniment, ils ne contiennent pas de données nominatives et constituent la mémoire institutionnelle de l'établissement

- **Logs email** : conservation 12 mois, suppression automatique au-delà
- **Données de facturation** : 10 ans (obligation comptable)
- **Données techniques de fonctionnement** : envois en échec et erreurs techniques 30 jours glissants ; sessions jusqu'à leur expiration (8 heures) ; date de dernière connexion tant que le compte existe
- **Pièces jointes** : supprimées à la clôture de la crise si demandé

Un export RGPD et une fonction de purge manuelle sont disponibles via le panneau administrateur (onglet RGPD).

2.6 Droits des personnes concernées

- **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

Ces droits s'exercent auprès du **responsable de traitement** (l'établissement abonné). Pour toute question relative à l'infrastructure technique : support@ifclubs.fr.

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

En cas de violation de données à caractère personnel, l'éditeur s'engage à notifier le responsable de traitement dans les **72 heures** suivant la prise de connaissance de l'incident, à documenter la violation dans un registre des incidents, à évaluer le risque pour les droits et libertés des personnes concernées, et à assister le responsable de traitement pour la notification à la CNIL si nécessaire.

Minimisation — niveau régional (26/09/2026) : les demandes d'aide d'un établissement ne transmettent au régional que l'**alias** de la personne (« Prénom I. »), jamais son nom complet, son email ou son téléphone ; les indicateurs de conformité et les exercices ne remontent que sous forme de **compteurs et de dates** ; le rapport périodique du régional ne contient aucune donnée nominative du personnel. Les saisies de téléphones et d'adresses sont contrôlées à la source (format, extension existante), ce qui évite l'envoi d'alertes à des destinataires erronés.

Marques de lecture (26/09/2026) : le bouton « Lu » enregistre, pour la seule personne concernée, les décisions et informations qu'elle a lues ; ces marques ne sont montrées à personne d'autre (ni la cellule, ni le régional, ni le groupe). **Appareils** : aucune réponse contenant des données de crise n'est conservée dans le cache du téléphone ou du navigateur. **Comptes retenus (27/09/2026)** : sur téléphone, la page de connexion garde localement l'email et le nom des comptes utilisés (6 au plus, jamais le mot de passe, rien transmis au serveur), effaçables d'un appui long.

3. Sécurité réseau et infrastructure

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 — aucun HTTP en production
- **Certificat wildcard unique (19/09/2026)** : un seul certificat (*.crise.ifclubs.fr) couvre tous les établissements, au lieu d'un certificat individuel par établissement — empêche la divulgation de la liste des clients via les journaux publics de transparence des certificats (Certificate Transparency), un registre permanent et consultable par quiconque, indépendant de la sécurité applicative

3.2 Authentification et contrôle d'accès

Deux modes de connexion coexistent dans le logiciel, tous deux fondés sur un compte individuel par personne (plus de mot de passe partagé entre plusieurs utilisateurs d'un même rôle) ; chaque établissement choisit le sien depuis sa console d'administration :

- **Mode par défaut — Identifiant (email) + mot de passe personnel** : chaque utilisateur se connecte avec son adresse email et un mot de passe personnel (12 caractères minimum, lettre + chiffre + caractère spécial), haché bcrypt (coût 10). Récupération par mot de passe temporaire à usage unique (10 minutes), envoyé par email ou SMS.
- **Mode renforcé — Identité + code TOTP** (Google/Microsoft Authenticator) : code rotatif à 6 chiffres (RFC 6238), secret d'enrôlement chiffré au repos (AES-256-GCM), jamais stocké en clair sur le serveur.

Séparation stricte des rôles (admin / membre / invité) appliquée côté serveur sur chaque route, jamais côté client uniquement — le rôle est désormais déduit automatiquement du compte reconnu (email ou identité), sans déclaration manuelle par l'utilisateur. Limiteur de tentatives de connexion (fenêtre glissante de 15 minutes) sur l'ensemble des routes d'authentification, prévention brute force. Isolation stricte par tenant : chaque établissement n'accède qu'à ses propres données, y compris via la passerelle générale d'accès multi-établissements (crise.ifclubs.fr) qui ne conserve ni ne compare aucune donnée d'un établissement — chaque tentative de connexion est relayée en temps réel, sans base de données inter-établissements. Identifiants de sous-domaine opaques (non porteurs du nom du client) pour tout établissement, réduisant l'exposition résiduelle par indication de nom de serveur (SNI) lors de l'établissement d'une connexion HTTPS. Rappel RGPD affiché avant tout accès à la main courante, acquitté explicitement par l'utilisateur ("J'ai compris") — mesure organisationnelle de prévention contre la saisie de données de santé nominatives.

3.3 Headers de sécurité HTTP

- 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 **stricte, appliquée** sur toutes les interfaces depuis le 24/09/2026 : default-src 'self', script-src 'self', script-src-attr 'none', object-src 'none', base-uri, form-action, frame-ancestors — aucun script ni gestionnaire d'événement intégré aux pages (actions exécutées par un interpréteur sans eval, limité à une liste blanche)

3.4 Protection de l'infrastructure et des données au repos

MESURE	ÉTAT
Pare-feu (ufw, deny par défaut, ports 22/80/443 uniquement)	✓ Actif
EDR comportemental CrowdSec + auditd + fail2ban	✓ Actif
SSH : clé cryptographique uniquement, mot de passe désactivé, connexion root interdite, comptes nominatifs	✓ Actif
Un compte système non privilégié par établissement (isolation des fichiers entre clients)	✓ Actif
Environnement Node.js 24 LTS maintenu, dépendances sans vulnérabilité connue (npm audit)	✓ Actif
Jetons de session : seule leur empreinte SHA-256 est enregistrée ; déconnexion effective côté serveur	✓ Actif
Emails groupés en copie cachée (aucun destinataire ne voit les adresses des autres)	✓ Actif
Mises à jour de sécurité automatiques (unattended-upgrades)	✓ Actif
Sauvegardes chiffrées AES-256, clé dédiée par établissement, rétention 30 jours	✓ Actif
Fichiers de configuration sensibles (.env) en permissions 600, non versionnés	✓ Actif
Données au repos (fichiers JSON) : chiffrement au niveau bloc du système de fichiers	⚠ Roadmap
Intégrité des fichiers (hash SHA-256 à l'écriture/sauvegarde, contrôle admin sur demande)	✓ Actif

3.5 Validation et contrôle des entrées

- Validation du type MIME et de la signature binaire réelle des fichiers uploadés (PDF, images, documents)
- Limites de taille : 20 Mo (pièces jointes), 50 Mo (relevés PDF), 2 Mo par requête JSON (15 Mo pour l'enregistrement d'une crise, les transcriptions, RETEX et imports)
- Protection contre l'injection de commande : appels de processus sans interprétation shell (execFileSync) pour les scripts d'import
- Validation JSON stricte sur toutes les routes API
- Protection CORS : whitelist limitée à *.crise.ifclubs.fr
- Scanner de risques à l'intégration (20/07/2026) : tout PDF déposé dans le plan blanc ou la base documentaire est analysé **localement, sans aucun appel IA** (expressions déterministes) à la recherche de marqueurs de classification restreinte/interne, mobiles personnels et emails nominatifs — comportement bloquant par défaut (paramétrable en avertissement par

établissement) ; s'ajoute une validation humaine obligatoire par un Valideur dans la base documentaire avant tout traitement IA — cette validation conditionne aussi l'usage du plan blanc et des fiches réflexes par l'IA, via un document au nom correspondant approuvé par un Valideur

- Scanner de risques sur texte libre (20/07/2026) : même principe, appliqué **localement, sans aucun appel IA**, au journal de crise (à chaque saisie), aux transcriptions de réunion (à l'import) et aux messages externes soumis au résumé IA — recherche de mobiles personnels, emails nominatifs et numéros de sécurité sociale (NIR), comportement bloquant par défaut, paramétrable en avertissement par établissement, indépendamment pour chaque flux
- Dictée vocale désactivable (20/07/2026) : la reconnaissance vocale du navigateur fait transiter l'audio par un service tiers (ex. Google sur Chrome) avant que le texte ne nous parvienne — une caractéristique normale, inhérente à cette technologie ; le texte reconnu est ensuite soumis au même scan de pré-envoi que toute entrée du journal, dictée ou tapée. Un établissement peut désactiver entièrement la dictée depuis son panneau admin pour ne conserver que la saisie clavier

3.6 Disponibilité et continuité de service

- Monitoring automatique toutes les 5 minutes (services, sites, ressources, bande passante, certificats, sauvegardes, liaisons WhatsApp de chaque établissement), redémarrage automatique en cas d'indisponibilité, alerte immédiate de l'équipe support
- Support proactif : l'éditeur est prévenu automatiquement si une alerte de crise n'a pas pu être délivrée (en urgence pendant une crise), si un utilisateur rencontre une erreur technique, ou si le contrôle automatique nocturne détecte une anomalie — les emails reçus par l'éditeur ne contiennent aucune information identifiant le client
- Continuité des sessions : une maintenance ne déconnecte pas les utilisateurs
- Bilan de santé consultable par l'établissement dans son administration (liaisons d'alerte, équipe, exercices, retours d'expérience, abonnement), avec conseils
- Log d'audit append-only traçant toutes les ouvertures/fermetures/suppressions de crise
- Processus Node.js géré par systemd (redémarrage automatique au boot)
- RPO (perte de données maximale) : 24h · RTO (délai de restauration) : 4h ouvrées maximum

3.7 Gestion des sous-traitants ultérieurs

SOUS-TRAITANT	LOCALISATION	USAGE	GARANTIES RGPD
IONOS SE (hébergement)	France (UE)	VPS mutualisé, stockage	Certifié ISO 27001, DPA disponible — pas de transfert hors UE
Mistral AI (défaut)	France (UE)	Synthèse, conseils, RETEX	DPA disponible, pas d'entraînement de modèle, hébergement UE par défaut
Groq Inc. (optionnel)	États-Unis	Synthèse, conseils — activable par le client à la place de Mistral	DPA disponible, CCT/SCC, rétention 0 jour (traitement mémoire)
Anthropic PBC (optionnel)	États-Unis	Synthèse, RETEX approfondi — activable par le client ; synthèses régionales et nationales automatiques	DPA disponible, CCT/SCC, rétention 30 jours max (logs sécurité)
Azure OpenAI (optionnel)	Déploiement du client	IA — sous le tenant M365 propre du client	Couvert par le contrat Microsoft du client
Meta (WhatsApp)	États-Unis	Notifications crise (best-effort)	CGU WhatsApp Business — voir note ci-dessous
Scaleway SAS (optionnel)	France (UE)	Alertes SMS, niveau régional uniquement	Intra-UE, désactivé par défaut, désactivable à tout moment
Fournisseur SMTP	Variable	Envoi d'emails de notification	Configuré et choisi par l'établissement — sous sa responsabilité

Note WhatsApp : l'intégration WhatsApp utilise actuellement une librairie d'automatisation non officielle. Elle est mentionnée dans les CGV comme fonctionnalité "best-effort" — susceptible d'être interrompue sans préavis par Meta. Une migration vers l'API officielle WhatsApp Business Cloud est prévue à l'entrée du premier client nécessitant une garantie contractuelle sur ce canal. Les établissements souhaitant une conformité stricte peuvent désactiver cette fonctionnalité.



Une triple surveillance au service de nos clients

Chez REACTis, notre objectif est simple : **détecter et corriger une anomalie avant même que vous ayez à nous la signaler.** Pour cela, nos équipes s'appuient sur trois niveaux de surveillance complémentaires, actifs en permanence.

1. Surveillance des serveurs, jour et nuit

L'état de nos serveurs est contrôlé automatiquement toutes les 5 minutes (services, sites, ressources). Chaque nuit, un bilan de santé complet est adressé à nos équipes : le moindre signe de faiblesse est repéré avant d'avoir un effet sur votre service.

2. Alertes proactives sur votre espace

Dès qu'un élément de votre espace ne fonctionne pas comme prévu, nos équipes sont alertées automatiquement. Par exemple :

- la liaison d'alerte WhatsApp est interrompue ;
- les relevés automatiques ne sont plus reçus ;
- un message n'a pas pu être délivré ;
- une adresse e-mail saisie est invalide.

Selon les cas, nous corrigeons directement, ou nous vous indiquons précisément quoi faire, et qui dans votre établissement peut le faire.

3. Remontée des erreurs techniques

Si un utilisateur rencontre une erreur technique pendant qu'il utilise REACTis, elle nous est remontée automatiquement. Nos équipes l'analysent, la corrigent, puis la retirent de leur suivi. Ces remontées sont anonymisées : elles décrivent l'erreur, jamais le contenu de vos crises ni l'identité des personnes.

Le résultat : une plateforme fiable, surveillée en continu, où la plupart des anomalies sont réglées avant que vous ne les remarquiez.

4. Cadre légal et contractuel

4.1 Documents légaux disponibles sur la plateforme

- Conditions Générales de Vente (CGV) : </cgv.html>
- Conditions Générales d'Utilisation (CGU) : </cgu.html>
- Data Processing Agreement (DPA) : </dpa.html>
- Politique de confidentialité (RGPD) : </rgpd.html>
- Registre des traitements Art. 30 : </registre-traitements.html>
- Politique de Sécurité des Systèmes d'Information (PSSI) : </pssi.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 : informations sur les ressources disponibles (lits, effectifs, matériel — données non nominatives), messages de coordination entre membres de la cellule (données nominatives des professionnels), notifications à des contacts institutionnels (ARS, SAMU, partenaires — coordonnées professionnelles).

La plateforme **ne traite pas** de données de santé nominatives des patients. Afin de prévenir toute saisie involontaire, un message d'alerte est affiché à chaque connexion : 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 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. Si un établissement venait à inclure de telles données dans la main courante malgré le rappel affiché à la connexion, l'éditeur devrait être certifié HDS.

Point à assumer : l'hébergement actuel repose sur un VPS mutualisé IONOS (ISO 27001), non sur un serveur OVH dédié certifié HDS. Cette certification n'est pas une obligation réglementaire pour ce périmètre, mais une migration vers un hébergeur OVH dédié certifié HDS est planifiée (S1 2027), par choix de renforcement plutôt que par obligation.

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, permettant de valider l'opérationnalité du dispositif : exercices de simulation (plans blancs, canicule, incidents techniques) conduits avec succès, crises réelles pilotées avec traçabilité complète de la main courante et notification multi-canal, rapports RETEX générés automatiquement et validés par les établissements participants. 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 par défaut et peuvent être exportées ou purgées à la demande. Un log d'audit indépendant trace toutes les actions administratives. Les sauvegardes chiffrées garantissent la pérennité des archives de crise.

6. Contacts et responsabilités

Éditeur et propriétaire de la plateforme : IFClubs SAS, représentée par Frédéric Taillez — support@ifclubs.fr

Responsable de traitement : l'établissement client utilisateur de la plateforme (responsable de traitement au sens du RGPD Art. 4), identifié dans son contrat d'abonnement.

Délégué à la Protection des Données (DPO) : 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).

