Contrat de Licence Utilisateur Final (CLUF / CGU)

Version	Contributeur	Date de publication	Date de validité	Commentaires
4.0	LM	1er août 2026	31 août 2026	Refonte
3.0	LM	7 janvier 2022	1er mars 2022	Ajustements : formation (Art5)
2.0	LM	5 juillet 2018	5 septembre 2018	Version commerciale

Sommaire

ARTICLE 1. OBJET, NATURE CONTRACTUELLE, OPPOSABILITE ET HIERARCHIE 2
ARTICLE 2. DEFINITIONS 2
ARTICLE 3. CONCESSION DE DROITS D'UTILISATION ET PREREQUIS 2
ARTICLE 4. FORMATION, HABILITATION ET CANAL DE SUPPORT 3
ARTICLE 5. OBLIGATIONS, SECURITE ET RESPONSABILITES DE L'UTILISATEUR 4
ARTICLE 6. PROPRIETE INTELLECTUELLE ET FEEDBACKS 5
ARTICLE 7. DONNEES A CARACTERE PERSONNEL, SECURITE ET FLUX TIERS 5
ARTICLE 8. ÉVOLUTIONS, MODE DEGRADE ET OBSOLESCENCE 6
ARTICLE 9. DISPOSITIONS DIVERSES ET REVISION 6
Annexe A : DPA — Accord sur le Traitement des Données Personnelles et de Santé (Art. 28 RGPD)
Article 1. Objet et Qualification Juridique des Rôles 7
Article 2. Description du Traitement 7
Article 3. Obligations de CrisiSoft (Sous-traitant) 7
Article 4. Sécurité et Hébergement HDS 8
Article 5. Sous-traitance ultérieure 8
Article 6. Droits des personnes concernées 8
Article 7. Notification des violations de données 8
Article 8. Sort des données (Réversibilité et Purge) 9
Article 9. Registre et Audit 9

ARTICLE 1. OBJET, NATURE CONTRACTUELLE, OPPOSABILITE ET HIERARCHIE

Les présentes Conditions Générales d'Utilisation (ci-après « **CGU** » ou « **CLUF** ») régissent l'accès et l'utilisation de la Solution applicative de gestion de crise « **MenKorn** » (ci-après la « **Solution** ») éditée par **CrisiSoft SAS**.
Elles s'imposent de plein droit à tout Organisme bénéficiaire et à tout Utilisateur, que l'accès à la Solution soit souscrit directement auprès de CrisiSoft ou par l'intermédiaire d'une centrale d'achat, d'un groupement d'achat public ou de tout autre intermédiaire commercial (ci-après le « Client »).
L'accès à la Solution ou sa première utilisation par un Utilisateur vaut acceptation sans réserve du présent CLUF/CGU par l'Organisme et ses Utilisateurs.
Elles s'inscrivent dans le cadre de la **Liasse Contractuelle** indivisible liant le Client et l'Organisme à CrisiSoft, aux côtés du Bon de Commande, des **Conditions Générales de Vente (CGV)** et de la **Convention de Niveaux de Service (SLA & Support)**.
L'accès et l'utilisation de la Solution par l'Utilisateur valent acceptation sans réserve du présent CLUF/CGU et du respect des règles de sécurité et d'usage de la Solution, à l'exclusion des dispositions commerciales des **Conditions Générales de Vente (CGV)** qui s'imposent exclusivement au Client payeur et à l'Organisme contractant.
Ordre de Priorité Contractuelle : En cas de contradiction ou de divergence entre les dispositions des documents constituant la Liasse Contractuelle, l'ordre de prévalence suivant s'appliquera stricto sensu :

1. Le **Bon de Commande / Devis** (stipulations particulières)
2. La **Convention de Niveaux de Service** (SLA & Support)
3. **L'Annexe A : DPA** (Accord sur le Traitement des Données annexé au Contrat de Licence Utilisateur Final (CLUF / CGU))
4. Les présentes **Conditions Générales de Vente** (CGV)
5. Le **Contrat de Licence Utilisateur Final** (CLUF / CGU).

ARTICLE 2. DEFINITIONS

Pour l'interprétation des présentes, les termes définis ci-après ainsi que ceux figurant dans l'Article 2 des **Conditions Générales de Vente (CGV)** de CrisiSoft s'appliquent :

- « Client » désigne la personne morale (centrale d'achat, intermédiaire commercial, ou établissement) qui passe commande auprès de CrisiSoft et assume la responsabilité financière des redevances.
- « Organisme » désigne l'établissement de santé, la structure publique ou privée (ex: CHU, SAMU, SDIS) destinataire effective, déployant et exploitant la Solution pour ses besoins de gestion de crise. Le Client et l'Organisme peuvent désigner la même entité.
- « Utilisateur » désigne toute personne physique autorisée par l'Organisme à accéder à la Solution sous ses identifiants personnels et nominatifs.
- « Référent » désigne un Utilisateur ayant suivi avec succès le parcours de formation initiale délivré par CrisiSoft, seul habilité à former d'autres Utilisateurs en interne et à jour de ses obligations de recyclage annuel.

ARTICLE 3. CONCESSION DE DROITS D'UTILISATION ET PREREQUIS

3.1. Périmètre de la Licence

CrisiSoft concède à l'Utilisateur et à l'Organisme un droit d'accès et d'utilisation de la Solution, personnel, non exclusif, non cessible et non transférable. Ce droit est strictement limité :

1. À l'usage professionnel de l'Utilisateur pour le compte de l'Organisme désigné au Bon de Commande (à l'exclusion de tout autre établissement membre d'un même Groupement non expressément visé) ;
2. À la durée de validité du contrat souscrit par le Client pour le compte de l'Organisme ;
3. Au respect des « Unités d'Œuvre » (ex: nombre de comptes, lits, structures) définies au Bon de Commande.

Tout usage dépassant ces limites ou toute tentative de rétro-ingénierie, décompilation ou modification de la Solution est strictement interdit.

3.2. Prérequis Techniques et Environnement Utilisateur

L'accès opérationnel à la Solution nécessite le respect par le Client, l'Organisme et l'Utilisateur des prérequis techniques matériels, logiciels, d'infrastructure et de réseau minimaux figurant dans les **« Prérequis Techniques »** du document **Convention de Niveaux de Service (SLA & Support)**.
L'Utilisateur et l'Organisme demeurent seuls responsables du maintien en bon état de fonctionnement de leurs postes de travail et de leur infrastructure télécom. CrisiSoft ne saurait être tenue pour responsable d'un défaut d'accès ou d'une dégradation des performances résultant du non-respect de ces prérequis techniques répertoriés à la **Convention de Niveaux de Service (SLA & Support)**.

3.3. Capacité Juridique et Habilitation

L'Utilisateur déclare agir dans le cadre exclusif de ses fonctions professionnelles et être dûment habilité par l'Organisme à accéder à la Solution. Il déclare à ce titre disposer de la pleine capacité juridique pour accepter les présentes CLUF / CGU, c'est-à-dire avoir la majorité légale et ne faire l'objet d'aucune mesure de protection juridique des majeurs (mise sous sauvegarde de justice, sous curatelle ou sous tutelle).

ARTICLE 4. FORMATION, HABILITATION ET CANAL DE SUPPORT

4.1. Statut de Référent et Habilitation aux Paramétrages

Seuls les Utilisateurs ayant validé le parcours de formation initiale délivré par CrisiSoft disposent du statut de **Référent** et sont les seuls habilités à former d'autres Utilisateurs au sein de leur Organisme.
Les Utilisateurs ayant été régulièrement formés par un Référent interne sont autorisés à utiliser la Solution ainsi qu'à réaliser les paramétrages opérationnels autorisés par leurs droits d'accès.

4.2. Recyclage Annuel Obligatoire du Référent

Pour garantir la sécurité opérationnelle et le maintien de la conformité réglementaire de la Solution, chaque Référent doit réaliser un recyclage annuel dispensé par CrisiSoft.
Conséquence opérationnelle : La perte de validité du recyclage annuel entraîne la suspension immédiate du statut de Référent. Cette suspension est notifiée par CrisiSoft et entraîne, conformément aux **Conditions Générales de Vente (CGV)**, la suspension des prestations d'accompagnement et de suivi opérationnel associées au niveau de l'Organisme, sans droit à indemnité pour le Client ni pour l'Organisme.

4.3. Canal de Support Opérationnel, Filtrage et Plages Horaires

L'assistance technique, le support applicatif et la hotline sont assurés **directement entre CrisiSoft et les équipes de l'Organisme**. Aucun intermédiaire commercial ou centrale d'achat n'est habilité à s'immiscer dans le traitement des demandes techniques.

Règles de Sollicitation et Canaux (Filtrage) : Afin d'éviter la saturation des équipes d'intervention de CrisiSoft, l'Utilisateur et l'Organisme s'engagent à respecter le filtrage suivant :

- **Niveau 0 (Base de Connaissances) : Avant toute sollicitation du support technique, le Référent de l'Organisme s'engage à consulter la Base de Connaissances (FAQ, tutoriels, vidéos)** mise à sa disposition sur le site web support, documentant le fonctionnement nominal de la Solution
- **Le Portail Web de Support (Ticketing) :** Canal unique et obligatoire pour les questions d'usage, le paramétrage, les demandes d'évolution ou les signalements d'anomalies mineures.
- **La Ligne Téléphonique (Hotline) : Son usage est strictement réservé aux signalements d'incidents techniques majeurs ou bloquants (Sévérité A et B) survenant en « Situation Réelle » de crise.** Les appels pour des anomalies mineures ou pour des situations d'exercice/simulation seront refusés et réorientés vers le portail de ticketing.
  Afin de garantir un traitement prioritaire des urgences, l'accès direct par téléphone aux prestations de support est prioritairement réservé aux **Référents** de l'Organisme à jour de leur recyclage annuel. Les demandes émanant d'Utilisateurs non Référents seront majoritairement réorientées vers les Référents internes de leur établissement et réalisées sur le portail web de support via les formulaires de demande.

Exclusion pour les Offres Simplifiées : L'accès à l'assistance téléphonique (Hotline) est strictement exclu pour les abonnements aux solutions simplifiées commercialisées directement en ligne par CrisiSoft. Pour ces offres spécifiques, le support technique et l'assistance s'effectuent exclusivement de manière asynchrone via le Portail Web de Support (Ticketing).

Plages Horaires Standard et Option Hotline 24/7 : Les prestations de support et la hotline sont accessibles par défaut pendant les **Jours et Horaires Ouvrés (JHO)** indiqués au document **Convention de Niveaux de Service (SLA & Support)**. L'accès étendu au support 24 heures sur 24 et 7 jours sur 7 (Option Hotline 24/7) constitue une prestation optionnelle soumise à souscription expresse au Bon de Commande.

Modalités Particulières pour les Sollicitations Hors Heures Ouvrées (sans Option 24/7) : Lorsque l'Organisme ou ses Utilisateurs contactent la hotline ou sollicitent les équipes de support de CrisiSoft en dehors des Jours et Horaires Ouvrés sans être titulaires de l'Option Hotline 24/7 en vigueur, les règles suivantes s'appliquent de plein droit :

1. **Anomalie Bloquante Majeure / Incident Système Global :** Si la sollicitation concerne une panne système lourde, une indisponibilité totale de la plateforme applicative ou un incident technique bloquant impactant la collectivité des usagers, la demande est prise en charge par CrisiSoft à titre de maintenance préventive et de supervision globale, sans surcoût pour l'Organisme.
2. **Demande d'Assistance Fonctionnelle, d'Usage ou Incident Non Bloquant :** Toute intervention, réponse ou assistance apportée par les équipes de CrisiSoft Hors Heures Ouvrées portant sur une demande d'usage, de formation, de paramétrage, d'assistance opérationnelle ou sur une anomalie non bloquante fera l'objet d'une **facturation spécifique d'intervention d'astreinte hors contrat** adressée au Client ou à l'Organisme, calculée sur la base du tarif horaire Hors Heures Ouvrées (HHO) en vigueur figurant au catalogue de CrisiSoft.

ARTICLE 5. OBLIGATIONS, SECURITE ET RESPONSABILITES DE L'UTILISATEUR

5.1. Nominalité Stricte et Interdiction des Comptes Partagés

Chaque compte Utilisateur est strictement individuel, personnel et nominatif. Pour garantir la traçabilité légale, l'imputabilité des décisions enregistrées dans la main courante de crise et la conformité au RGPD/HDS, **la création et l'usage de comptes partagés, génériques ou collectifs (ex: gardecrise@chu.fr, poste_samu@centre15.fr) sont strictement interdits.** CrisiSoft ne saurait en aucun cas être tenue pour responsable de l'utilisation de tels comptes.
L'Utilisateur s'engage à maintenir la confidentialité absolue de ses identifiants de connexion et à ne les communiquer à aucun tiers.
Dérogation pour les Offres Simplifiées (Souscription en ligne) : Par exception stricte à la règle de nominalité visée au paragraphe précédent, certaines versions simplifiées de la Solution commercialisées spécifiquement en ligne par CrisiSoft reposent par conception sur l'attribution d'un compte utilisateur unique et partagé pour l'Organisme. Dans ce cas de figure exclusif, l'Organisme assume l'entière et pleine responsabilité des actions effectuées sous ce compte générique. L'Organisme fait son affaire de la traçabilité interne des agents utilisant ce compte et décharge expressément CrisiSoft de toute responsabilité quant au défaut d'imputabilité individuelle des actions enregistrées dans la main courante applicative.

5.2. Usage Conforme et Contenus

L'Utilisateur s'engage à utiliser la Solution exclusivement pour les besoins de gestion de crise de l'Organisme, et à ne pas introduire de données illicites, malveillantes ou portant atteinte aux droits de tiers. Toute utilisation artificielle d'un compte CrisiSoft ou de la Solution via des processus automatisés (tels que des robots ou des scripts) ou par tout autre moyen est strictement interdite.

5.3. Signalement d'Anomalie et Incident de Sécurité sous 24h

L'Utilisateur ou l'Organisme s'engage à notifier à CrisiSoft, **sans délai et au plus tard dans un délai de vingt-quatre (24) heures**, toute perte, vol, suspicion de compromission de ses identifiants de connexion ou toute vulnérabilité de sécurité constatée sur la Solution.

5.4. Exclusion de Responsabilité sur les Actes de Gestion de Crise

La Solution MenKorn constitue un outil logiciel d'aide à la décision, d'organisation des dispositifs de crise et de main courante informatique. La prise de décision opérationnelle, la conduite des opérations et la gestion des événements de crise relèvent de la responsabilité exclusive des autorités administratives et opérationnelles de l'Organisme.
CrisiSoft ne saurait en aucun cas être tenue pour responsable des dommages corporels, matériels, directs ou indirects, résultant d'une décision de crise, d'un arbitrage ou d'une consigne opérationnelle ordonnée par l'Utilisateur ou l'Organisme via la Solution.

5.5. Sanctions en cas de Manquement

Sans préjudice de tous dommages et intérêts que CrisiSoft pourrait solliciter, CrisiSoft se réserve le droit de suspendre l'accès d'un Utilisateur et/ou de l'Organisme à la Solution, et/ou de résilier de plein droit, sans préavis ni indemnité, son inscription à la Solution MenKorn en cas de :

- Non-respect par l'Utilisateur ou l'Organisme des présentes conditions générales d'utilisation, et notamment :
  - Non-respect des droits de propriété intellectuelle de CrisiSoft et/ou de ses concédants ;
  - Contournement ou tentative de contournement des mesures techniques de protection mises en place par CrisiSoft ;
  - Fourniture de fausses informations lors de son inscription ou de son habilitation à la Solution MenKorn ;
- Agissements contraires aux intérêts commerciaux de CrisiSoft.

ARTICLE 6. PROPRIETE INTELLECTUELLE ET FEEDBACKS

6.1. Droits d'Auteur

La Solution MenKorn, ses algorithmes, son architecture, ses interfaces et ses documentations sont la propriété exclusive de CrisiSoft. L'accès à la Solution ne confère aucun droit de propriété intellectuelle à l'Utilisateur ni à l'Organisme. Toute représentation totale ou partielle de la Solution et/ou des éléments la composant par quelque procédé que ce soit, sans l'autorisation expresse de CrisiSoft, est dès lors interdite et constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

6.2. Droit d'Exploitation des Feedbacks et Télémétrie Anonymisée

L'Utilisateur et l'Organisme cèdent à CrisiSoft, à titre gratuit et non exclusif, le droit d'utiliser l'ensemble des suggestions, retours d'expérience, demandes d'amélioration et remarques émis concernant la Solution (les « Feedbacks »). CrisiSoft pourra librement intégrer ces Feedbacks dans ses développements futurs sans restriction ni redevance.
De même, CrisiSoft est autorisée à collecter et traiter des données d'usage techniques (télémétrie) sous forme **strictement anonyme et agrégée** à des fins d'optimisation des performances, d'analyse statistique et d'amélioration continue de ses algorithmes.

ARTICLE 7. DONNEES A CARACTERE PERSONNEL, SECURITE ET FLUX TIERS

7.1. Protection des Données, HDS, Qualification RGPD et DPA Direct

Qualification des Rôles : L'Organisme qualifie et demeure seul **Responsable de Traitement** au sens du RGPD pour l'ensemble des données des personnels, agents et données de santé (HDS) traitées via la Solution. CrisiSoft agit exclusivement en qualité de **Sous-traitant** sur instructions documentées de l'Organisme, conformément à l'Article 28 du RGPD.
Étanchéité vis-à-vis du Client / Centrale d'Achat : Lorsque le contrat est souscrit via un Client intermédiaire ou une centrale d'achat, ce dernier n'a la qualité ni de Responsable de Traitement ni de Sous-traitant au sens du RGPD. Le Client intermédiaire n'a aucun accès aux données personnelles, aux données opérationnelles, mains courantes de crise ou données de santé traitées par l'Organisme via la Solution.
Formalisation du DPA (Art. 28.3 RGPD) : Les engagements de CrisiSoft en matière de traitement des données, de sécurité Cloud HDS, de notification des violations sous 24h/48h et de sous-traitance ultérieure sont régis de manière autonome par l'**« Annexe A : DPA — Accord sur le Traitement des Données »** intégrée aux présentes CLUF / CGU.
Acceptation Directe et Opposabilité : L'accès à la Solution par le Référent ou l'Administrateur de l'Organisme, ou la validation de la Fiche de Raccordement de Déploiement, vaut acceptation expresse et conclusion directe de l'Annexe A (DPA intégrée aux présentes CLUF / CGU) entre l'Organisme (Responsable de Traitement) et CrisiSoft (Sous-traitant), indépendamment du canal de souscription commercial (Centrale d'achat).
En cas de fin de contrat, la réversibilité et la restitution des données sont effectuées par CrisiSoft directement au bénéfice exclusif de l'Organisme.
L'Utilisateur s'engage à respecter les règles d'authentification forte recommandées par l'Organisme.

7.2. Fiabilité et Exactitude des Flux de Données Tiers

La Solution peut intégrer des flux d'informations et services fournis par des tiers (APIs météo, données cartographiques, flux d'alertes sanitaires, réseaux télécoms). CrisiSoft ne saurait être tenue pour responsable de l'inexactitude, des retards, des interruptions ou des erreurs contenus dans ces données d'origine externe, sur lesquelles elle n'exerce aucun contrôle direct.

ARTICLE 8. ÉVOLUTIONS, MODE DEGRADE ET OBSOLESCENCE

8.1. Évolutions de la Solution

CrisiSoft se réserve le droit de faire évoluer la Solution pour des raisons fonctionnelles, techniques, réglementaires ou de sécurité.

8.2. Fonctionnement en Mode Dégradé et Continuité d'Activité

En cas de crise majeure entraînant une rupture des réseaux télécoms publics ou de la connectivité Internet globale, la Solution peut basculer sur des modes de fonctionnement dégradés (SMS, relais satellite, stockage en cache local). L'Utilisateur et l'Organisme sont informés que certaines fonctionnalités avancées peuvent être temporairement restreintes ou suspendues pendant la durée du Mode Dégradé.
CrisiSoft garantit l'intégrité des données saisies localement et leur resynchronisation dès le rétablissement des communications, sans que le fonctionnement temporaire en Mode Dégradé ne puisse constituer une inexécution contractuelle.

8.3. Obsolescence Matérielle

En cas d'évolution majeure rendant obsolète le matériel informatique de l'Organisme (prérequis techniques non respectés), CrisiSoft ne saurait être tenue pour responsable de l'altération des performances de la Solution.

8.4. Inexécution ou Résiliation du Contrat souscrit par le Client

L'accès de l'Organisme et de ses Utilisateurs à la Solution est strictement subordonné au maintien en vigueur du contrat souscrit par le Client (Centrale d'achat / Intermédiaire) auprès de CrisiSoft.
En cas de résiliation, de non-renouvellement du marché ou de défaut de paiement du Client, CrisiSoft sera fondée à suspendre ou interrompre l'accès à la Solution au niveau de l'Organisme, sans que ce dernier ni ses Utilisateurs ne puissent rechercher la responsabilité de CrisiSoft ou prétendre à une quelconque indemnité.

ARTICLE 9. DISPOSITIONS DIVERSES ET REVISION

9.1. Droit Applicable et Juridiction

Les présentes CLUF / CGU sont régies par le droit français. Tout litige relatif à leur exécution sera soumis à la compétence des tribunaux désignés dans l'Article 14 des **Conditions Générales de Vente (CGV)**.

9.2. Modalités de Révision Unilatérale des CLUF / CGU

CrisiSoft se réserve le droit de modifier le présent CLUF/CGU à tout moment pour refléter les évolutions légales, techniques ou opérationnelles de la Solution. Toute modification sera notifiée au Client, à l'Organisme et aux Utilisateurs par écrit (ou via une notification applicative) avec un préavis minimum de trente (30) jours avant sa prise d'effet. L'utilisation continue de la Solution à l'issue de ce délai vaut acceptation sans réserve des CLUF / CGU révisées.

Annexe A : DPA — Accord sur le Traitement des Données Personnelles et de Santé (Art. 28 RGPD)

Éditeur / Sous-traitant : CrisiSoft SAS
Solution : MenKorn
Statut du document : Cette Annexe A fait partie intégrante des Conditions Générales d'Utilisation (CGU / CLUF) de la Solution MenKorn. Elle vise à satisfaire aux exigences de l'Article 28.3 du Règlement Général sur la Protection des Données (RGPD).

Article 1. Objet et Qualification Juridique des Rôles

Le présent Accord sur le Traitement des Données (ci-après le « **DPA** ») a pour objet de définir les conditions dans lesquelles CrisiSoft s'engage à effectuer, pour le compte de l'Organisme client, les opérations de traitement de données à caractère personnel définies ci-après.
Dans le cadre de l'utilisation de la Solution MenKorn :

- L'**Organisme** (Établissement de santé, SAMU, SDIS, etc.) agit en qualité de **Responsable de Traitement** (RT).
- **CrisiSoft** agit exclusivement en qualité de **Sous-traitant** (ST).
- L'éventuelle **Centrale d'Achat** ou intermédiaire commercial intermédiaire n'a la qualité ni de Responsable de Traitement ni de Sous-traitant, et n'a aucun droit d'accès aux données traitées.

Article 2. Description du Traitement

Conformément aux instructions documentées par l'Organisme, notamment via la **« Fiche de Raccordement Technique & Mandat RGPD »**, CrisiSoft est autorisée à traiter les données pour les finalités suivantes :

2.1. Finalités du Traitement

1. Gestion opérationnelle des événements de crise, de garde et d'astreinte.
2. Mobilisation, alerte et suivi des effectifs et agents de l'Organisme.
3. Tenue automatisée de la main courante informatisée et traçabilité des décisions opérationnelles.

2.2. Catégories de Personnes Concernées

1. Tous personnels et agents sous la responsabilité de l'Organisme, ainsi que toute personne enregistrée dans le cadre de la gestion de crise.
2. Victimes et patients de l'événement de crise géré via la solution (si applicables au module) : Uniquement dans le cadre strict de l'organisation des dispositifs de crise et sous hébergement certifié HDS.

2.3. Catégories de Données Personnelles Traitées

- Identité & Métier : Nom, Prénom, Grade/Métier, Service d'affectation, Identifiants d'accès nominatifs.
- Coordonnées de Contact Professionnelles & Personnelles : Numéros de téléphone fixe/mobile, adresses postales, adresses email, identifiants de messagerie, identifiant professionnel.
- Données Télécoms & Logs : Journaux de connexion, logs d'horodatage des saisies dans la main courante, accusés de réception SMS/Appels.
- Données de Santé applicatives (si applicables au module) : Uniquement dans le cadre strict de l'organisation des dispositifs de crise et sous hébergement certifié HDS.

Article 3. Obligations de CrisiSoft (Sous-traitant)

CrisiSoft s'engage à :

1. **Instructions écrites :** Ne traiter les données que sur instruction documentée de l'Organisme. Si CrisiSoft est tenue de procéder à un transfert de données vers un pays tiers en vertu du droit de l'Union ou du droit français, elle en informera l'Organisme au préalable.
2. **Confidentialité :** Garantir que les personnes autorisées à traiter les données (employés, ingénieurs support) s'engagent à respecter la plus stricte confidentialité et reçoivent la formation nécessaire en matière de protection des données.
3. **Localisation :** Héberger et traiter l'intégralité des données exclusivement sur le territoire de l'Union Européenne.

Article 4. Sécurité et Hébergement HDS

CrisiSoft s'engage à mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.

Hébergement des Données de Santé (HDS) :

CrisiSoft garantit que les environnements de production hébergeant les données de la Solution MenKorn sont infogérés et stockés auprès d'un hébergeur disposant de la certification en vigueur relative à l'Hébergement de Données de Santé (HDS) couvrant l'intégralité des six (6) domaines d'activité d'hébergement et d'infogérance, conformément à l'article L.1111-8 du Code de la santé publique français. Les mesures incluent notamment le chiffrement des flux (TLS), le cloisonnement logique des bases de données par Organisme (étanchéité), et des politiques de sauvegardes régulières.

Article 5. Sous-traitance ultérieure

L'Organisme autorise CrisiSoft à faire appel à des sous-traitants ultérieurs (ci-après « Sous-traitant ultérieur ») pour mener des activités de traitement spécifiques.

Liste formelle des sous-traitants ultérieurs autorisés à la date des présentes :

Sous-traitant (Nom de la société)	Service ou Prestation fournie	Localisation des données
ADISTA	**Hébergement et Infogérance Cloud (Certifié HDS)**	**France métropolitaine**
DIGITAL VIRGO	**Routage des SMS d'alerte des personnels**	**France métropolitaine**
DIGITAL VIRGO	**Gestion des appels vocaux automatisés**	**France métropolitaine**
BREVO	**Routage des emails transactionnels**	**Union Européenne**

CrisiSoft informera l'Organisme (par e-mail ou notification applicative) de tout changement prévu concernant l'ajout ou le remplacement d'un Sous-traitant ultérieur. L'Organisme disposera d'un délai de quinze (15) jours pour émettre des objections légitimes. À défaut, le changement sera réputé accepté.

CrisiSoft impose à ses Sous-traitants ultérieurs les mêmes obligations de protection des données que celles fixées dans le présent DPA. CrisiSoft demeure pleinement responsable devant l'Organisme de l'exécution par le Sous-traitant ultérieur de ses obligations.

Article 6. Droits des personnes concernées

Il appartient à l'Organisme (Responsable de Traitement) de fournir l'information aux personnes concernées (ses agents) et de répondre à leurs demandes d'exercice de droits (accès, rectification, effacement, limitation).

Dans la mesure du possible, CrisiSoft assistera l'Organisme, par des mesures techniques et organisationnelles appropriées, pour s'acquitter de son obligation de donner suite à ces demandes. Si CrisiSoft reçoit une demande directe d'un agent de l'Organisme, elle ne répondra pas directement et transmettra cette demande au DPO de l'Organisme sans délai.

Article 7. Notification des violations de données

CrisiSoft notifie à l'Organisme toute violation de données à caractère personnel dans un délai maximum de **vingt-quatre (24) à quarante-huit (48) heures** après en avoir pris connaissance.

Cette notification, adressée au DPO ou à l'Administrateur de l'Organisme, est accompagnée de toute documentation utile afin de permettre au Responsable de Traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (CNIL) dans le délai légal de 72 heures.

Article 8. Sort des données (Réversibilité et Purge)

Au terme des relations contractuelles (fin du marché, non-renouvellement), CrisiSoft s'engage à restituer à l'Organisme (ou à un tiers désigné par lui), sur simple demande, l'ensemble de ses données dans un format structuré et couramment utilisé (Réversibilité).
À l'issue de cette réversibilité, ou à défaut de demande expresse de l'Organisme, CrisiSoft procèdera à l'**anonymisation irréversible** de l'ensemble des données à caractère personnel et données de santé.
Conformément à la doctrine de la CNIL et au considérant 26 du RGPD, cette anonymisation définitive vaut destruction légale des données à caractère personnel. L'Organisme autorise expressément CrisiSoft à conserver et traiter ces données purement statistiques et anonymes (volumétrie de crise, télémétrie) à des fins exclusives d'analyse et d'amélioration continue de la Solution MenKorn.

Article 9. Registre et Audit

CrisiSoft déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de ses clients.
CrisiSoft met à la disposition de l'Organisme toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent DPA. L'Organisme peut procéder, à ses frais et sous réserve d'un préavis de trente (30) jours, à un audit (sur pièces ou sur place par un tiers indépendant non concurrent de CrisiSoft et soumis à un accord de confidentialité) limité aux systèmes et locaux impliqués dans le traitement des données de l'Organisme.