# Accord de traitement des données clients

Contrat de sous-traitance au sens de l'article 28 du règlement (UE) 2016/679 (RGPD)
Annexe 3 des Conditions générales de vente de la plateforme cDESP

## Préambule

Le présent accord est conclu entre le Client, tel que défini dans les Conditions générales de vente cDESP (les « CGV »), agissant en qualité de **responsable de traitement**, et DCRR, Denquin & Ciatti Refrigeration Reglementary, société par actions simplifiée au capital de 1 000 euros, immatriculée au registre du commerce et des sociétés de Créteil sous le numéro 951 054 394, dont le siège social est situé 36 avenue Adrien Raynal, 94310 Orly, France (« **DCRR** »), agissant en qualité de **sous-traitant**.

Il fait partie intégrante des CGV et s'applique dès leur acceptation. Les termes commençant par une majuscule qui n'y sont pas définis ont le sens que leur donnent les CGV. Il s'inspire du modèle de clauses de sous-traitance publié par la Commission nationale de l'informatique et des libertés (CNIL). En cas de contradiction entre le présent accord et les CGV sur la protection des données à caractère personnel, le présent accord prévaut.

## Article 1. Définitions

- **Données Client** : les données à caractère personnel que le Client et ses Utilisateurs saisissent, importent, photographient, téléversent ou font générer dans l'Espace Client, ainsi que celles que la Plateforme transmet à des tiers à leur demande (par exemple un e-mail de rendez-vous adressé à un organisme habilité ou une demande de signature adressée à un contact du Client).
- **Espace Client** : l'ensemble des sites, groupes, équipements, contrôles, documents, rendez-vous, registres et messages rattachés au Client dans la Plateforme.
- **Sous-traitant ultérieur** : tout prestataire auquel DCRR confie tout ou partie du traitement des Données Client.
- **Violation de données** : une violation de la sécurité au sens de l'article 4, point 12, du RGPD touchant des Données Client.

## Article 2. Répartition des rôles

2.1. Pour les Données Client, le Client est responsable de traitement et DCRR est sous-traitant. Le Client détermine seul les finalités du traitement (suivi réglementaire de ses équipements sous pression et de ceux de ses propres clients, organisation de ses contrôles et de ses rendez-vous, archivage de ses documents) et décide des données qu'il y place.

2.2. DCRR est responsable de traitement, et le présent accord ne s'applique pas, pour les traitements qu'elle réalise pour son propre compte et qui sont décrits dans sa politique de confidentialité : création et gestion des comptes des Utilisateurs, authentification et sécurité, facturation et recouvrement, relation commerciale, support, mesure d'audience après consentement, amélioration du service à partir de statistiques agrégées, respect de ses obligations légales.

2.3. Lorsque DCRR réalise elle-même pour le Client une prestation de services réglementaires (inspection, contrôle, audit, dossier), cette prestation est régie par le contrat qui lui est propre. Le présent accord ne couvre que l'usage de la Plateforme.

## Article 3. Objet et description du traitement

DCRR est autorisée à traiter les Données Client pour le seul compte du Client, dans la mesure nécessaire à la fourniture de la Plateforme, à son hébergement, à sa sauvegarde, à sa maintenance et au support. La nature, la finalité, les catégories de données et de personnes concernées et la durée du traitement sont décrites à l'**annexe A**.

## Article 4. Durée

Le présent accord s'applique pendant toute la durée de la relation contractuelle entre le Client et DCRR, y compris pendant les périodes d'accès en lecture seule prévues aux CGV, puis jusqu'à l'exécution complète de l'article 13.

## Article 5. Instructions du Client

5.1. DCRR ne traite les Données Client que sur instruction documentée du Client, y compris pour les transferts vers un pays tiers, sauf obligation légale contraire ; dans ce cas, elle en informe le Client avant le traitement, sauf si la loi l'interdit.

5.2. Constituent les instructions du Client : les CGV, le présent accord et les actions réalisées par le Client et ses Utilisateurs dans la Plateforme (création, modification, envoi, signature, partage par groupe, export, suppression). Toute instruction complémentaire est donnée par écrit, y compris par e-mail à l'adresse indiquée à l'article 16.

5.3. DCRR informe immédiatement le Client si, selon elle, une instruction constitue une violation du RGPD ou d'une autre disposition du droit de l'Union ou des États membres relative à la protection des données.

5.4. DCRR n'utilise pas les Données Client pour ses propres finalités. En particulier, elle ne les vend pas, ne les utilise pas à des fins de prospection et ne les utilise pas pour entraîner des modèles d'intelligence artificielle.

## Article 6. Confidentialité

DCRR garantit la confidentialité des Données Client. Les personnes autorisées à les traiter, chez DCRR et chez ses Sous-traitants ultérieurs, sont soumises à une obligation de confidentialité et n'y accèdent que dans la mesure nécessaire à leur mission. Le personnel de DCRR n'accède au contenu de l'Espace Client que pour le support demandé par le Client, la maintenance, la sécurité ou une obligation légale.

## Article 7. Sécurité

DCRR met en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD. Ces mesures sont décrites à l'**annexe B**. DCRR peut les faire évoluer, à condition de ne pas réduire le niveau global de sécurité.

Le Client reste responsable de la sécurité de ce qui relève de lui : choix des Utilisateurs qu'il invite et des groupes auxquels il leur donne accès, confidentialité de leurs identifiants, retrait des accès des personnes qui quittent son organisation, sécurité de ses propres appareils.

## Article 8. Sous-traitants ultérieurs

8.1. Le Client donne à DCRR une autorisation générale de recourir aux Sous-traitants ultérieurs listés à l'**annexe C**. La liste à jour est publiée sur la page cdesp.app/sous-traitants.

8.2. DCRR informe le Client de tout ajout ou remplacement d'un Sous-traitant ultérieur au moins 30 jours à l'avance, par e-mail adressé à l'administrateur du compte du Client et par mise à jour de la page cdesp.app/sous-traitants, en précisant son identité, sa mission et le lieu du traitement. Dans ce délai, le Client peut s'y opposer par écrit pour un motif raisonnable lié à la protection des données. Les Parties cherchent alors une solution de bonne foi ; à défaut, le Client peut résilier son abonnement sans pénalité, avec effet au jour du changement, et obtient le remboursement de la part de l'abonnement déjà payée pour la période postérieure à la résiliation.

8.3. DCRR impose à chaque Sous-traitant ultérieur, par contrat, des obligations de protection des données au moins équivalentes à celles du présent accord. DCRR demeure pleinement responsable devant le Client de l'exécution de leurs obligations.

## Article 9. Transferts hors de l'Union européenne

9.1. Les Données Client, leurs fichiers et leurs sauvegardes sont stockés dans l'Union européenne.

9.2. Certains Sous-traitants ultérieurs sont établis hors de l'Union européenne ou peuvent y accéder ; c'est le cas de MXSoft LLC, société établie aux États-Unis qui assure l'exploitation technique de la Plateforme. Chaque transfert est encadré par l'une des garanties prévues au chapitre V du RGPD, indiquée pour chaque prestataire à l'annexe C : décision d'adéquation (notamment le cadre de protection des données UE-États-Unis pour les entreprises certifiées) ou clauses contractuelles types adoptées par la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021.

9.3. DCRR communique au Client qui le demande une copie des garanties applicables, le cas échéant expurgée des informations commerciales confidentielles.

## Article 10. Droits des personnes concernées

10.1. Il appartient au Client de répondre aux demandes des personnes concernées par les Données Client (accès, rectification, effacement, limitation, portabilité, opposition). La Plateforme lui permet de consulter, corriger, exporter et supprimer ces données.

10.2. DCRR aide le Client, par des mesures techniques et organisationnelles appropriées et dans la mesure du possible, à répondre à ces demandes lorsque les fonctions de la Plateforme ne suffisent pas.

10.3. Lorsqu'une personne s'adresse directement à DCRR au sujet de Données Client, DCRR transmet la demande au Client dans un délai de 5 jours ouvrés et n'y répond pas elle-même, sauf instruction du Client.

## Article 11. Violations de données

11.1. DCRR notifie au Client toute Violation de données dans les meilleurs délais et au plus tard 48 heures après en avoir pris connaissance, par e-mail adressé à l'administrateur du compte du Client.

11.2. La notification contient, dans la mesure du possible, les informations prévues à l'article 33, paragraphe 3, du RGPD : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées, coordonnées

d'un contact. Les informations non disponibles immédiatement sont communiquées dès que possible.

11.3. Il appartient au Client, en tant que responsable de traitement, de notifier la violation à l'autorité de contrôle et, le cas échéant, aux personnes concernées. DCRR l'y aide et ne procède elle-même à aucune notification relative aux Données Client sans instruction du Client, sauf obligation légale.

## Article 12. Assistance et documentation

DCRR aide le Client à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, notamment pour la réalisation d'analyses d'impact relatives à la protection des données et la consultation préalable de l'autorité de contrôle, compte tenu de la nature du traitement et des informations dont elle dispose. DCRR tient un registre des catégories d'activités de traitement effectuées pour le compte de ses clients, conformément à l'article 30, paragraphe 2, du RGPD.

## Article 13. Sort des données à la fin du contrat

13.1. La fin d'un abonnement n'entraîne pas la suppression des Données Client : conformément aux CGV, l'Espace Client passe en lecture seule et reste consultable et exportable.

13.2. Le Client peut à tout moment demander par écrit la clôture de son Espace Client. Avant la clôture, il peut exporter ses données au moyen des fonctions d'export de la Plateforme (archive ZIP des documents d'un site, exports PDF) ou demander à DCRR une restitution complète dans un format ouvert et couramment utilisé.

13.3. Après la clôture, DCRR supprime les Données Client de la base de production dans un délai de 30 jours, sauf obligation légale de conservation. Les copies contenues dans les sauvegardes chiffrées sont effacées au terme de leur cycle de rotation, au plus tard 13 mois après la clôture ; dans l'intervalle, elles ne sont utilisées pour aucune autre finalité que la restauration du service. DCRR confirme la suppression par écrit sur demande.

13.4. Les Données Client partagées avec d'autres utilisateurs par un groupe de sites, ou qui figurent dans des documents signés par des tiers, peuvent devoir être conservées pour ces autres utilisateurs ; DCRR en informe le Client et recherche avec lui la solution qui respecte les droits de chacun.

## Article 14. Audits

14.1. DCRR met à la disposition du Client les informations nécessaires pour démontrer le respect du présent accord, en priorité sous forme documentaire (description des mesures de sécurité, liste des Sous-traitants ultérieurs, réponses écrites à un questionnaire raisonnable).

14.2. Si ces informations ne suffisent pas, le Client peut faire réaliser un audit, y compris une inspection, par lui-même ou par un auditeur indépendant qu'il mandate et qui n'est pas un concurrent de DCRR, tenu à la confidentialité. Sauf Violation de données ou demande d'une autorité de contrôle, l'audit est annoncé au moins 30 jours à l'avance, n'a pas lieu plus d'une fois par an, est réalisé aux frais du Client, porte sur les seules Données Client et ne doit ni perturber le service ni donner accès aux données des autres clients.

## Article 15. Obligations du Client

Le Client :

- dispose d'une base légale pour chaque traitement qu'il réalise dans la Plateforme et informe les personnes concernées, notamment ses salariés, ses propres clients et leurs contacts, et les inspecteurs dont il saisit les coordonnées ;
- ne place dans la Plateforme aucune donnée sensible au sens des articles 9 et 10 du RGPD, ni aucune donnée sans rapport avec le suivi réglementaire de ses équipements ;
- veille à l'exactitude des données qu'il saisit et fixe leurs durées de conservation, en supprimant celles qui ne sont plus nécessaires ;
- donne à DCRR des instructions conformes au RGPD.

## Article 16. Contact

Toute question, instruction ou demande relative au présent accord est adressée à DCRR par e-mail à contact@dcrr.fr ou par la messagerie du support de la Plateforme (onglet « Équipe DCRR »).

## Article 17. Responsabilité, droit applicable et juridiction

Chaque Partie est responsable des dommages causés par sa violation du présent accord ou du RGPD dans les conditions de l'article 82 du RGPD. Dans les rapports entre les Parties, la responsabilité de DCRR au titre du présent accord est soumise aux limitations prévues par les CGV, sauf dans les cas où la loi interdit de la limiter. Le présent accord est régi par le droit français ; les litiges qui s'y rapportent relèvent de la juridiction désignée par les CGV.

## Annexe A. Description du traitement

| | |
|---|---|
| **Catégories de personnes concernées** | Utilisateurs invités par le Client (salariés, techniciens frigoristes, responsables de sites) ; clients du Client et leurs contacts ; exploitants et propriétaires des installations ; inspecteurs et organismes habilités dont le Client saisit les coordonnées ; signataires des documents ; personnes apparaissant de façon incidente sur les photos ou dans les documents téléversés. |
| **Catégories de données** | Identité et coordonnées professionnelles (nom, prénom, e-mail, téléphone, société, fonction) ; adresses des sites ; données techniques des sites et des équipements (non personnelles en elles-mêmes mais rattachées à ces personnes) ; dates et comptes rendus de contrôles et de rendez-vous ; signatures électroniques et leurs éléments de preuve (nom, date, adresse e-mail, code de vérification) ; documents, photos et plaques signalétiques ; registres de site ; messages échangés dans la Plateforme ; questions posées à l'assistant lorsqu'elles contiennent de telles données. |
| **Données sensibles** | Aucune. Le Client s'engage à n'en placer aucune (article 15). |
| **Nature des opérations** | Collecte par saisie, import ou téléversement, enregistrement, organisation, stockage, sauvegarde, consultation, modification, génération de documents PDF, lecture automatique de plaques signalétiques, recherche par l'assistant, envoi d'e-mails et de notifications à la demande du Client, export, suppression. |
| **Finalité** | Fournir au Client la Plateforme cDESP et ses fonctions de suivi réglementaire des équipements sous pression, en assurer la sécurité, la continuité, la sauvegarde et le support. |
| **Durée** | Durée de la relation contractuelle, puis article 13. |
| **Lieu de stockage** | Union européenne : Allemagne (Nuremberg) pour l'application et la base de données, Union européenne pour les fichiers, France pour la copie de secours. Accès d'administration depuis les États-Unis par MXSoft LLC (annexe C). |

## Annexe B. Mesures techniques et organisationnelles de sécurité

### Hébergement et réseau

- Serveurs de production chez Hetzner à Nuremberg (Allemagne) ; fichiers sur Cloudflare R2 dans la juridiction Union européenne.
- Base de données accessible uniquement depuis le réseau interne des conteneurs, jamais exposée sur internet.
- Chiffrement de toutes les communications (HTTPS/TLS) ; protection réseau et anti-robot par Cloudflare.
- Environnement de test séparé de la production : bases, stockage, identifiants et envois d'e-mails distincts ; aucune Donnée Client copiée en test.

### Contrôle d'accès

- Mots de passe stockés hachés (bcrypt) ; connexion possible par Google ou Apple ; vérification anti-robot à la connexion.
- Sessions limitées à 8 heures et à une seule session active par utilisateur.
- Rôles distincts ; un Utilisateur du Client n'accède qu'aux sites des groupes dont il est membre.
- Jetons d'accès au service de fichiers signés, valables 15 minutes ; vérification de l'appartenance au groupe du site avant tout accès à un fichier.
- Limitation du nombre de requêtes contre les abus.
- Accès d'administration aux serveurs par clés SSH, réservé à l'exploitant technique ; secrets conservés hors du code source.

### Disponibilité et sauvegardes

- Sauvegardes chiffrées de la base : horaires (conservées 2 jours), quotidiennes (30 jours), mensuelles (12 mois), et journal des opérations toutes les 5 minutes (14 jours) ; copie quotidienne chiffrée hors du serveur principal chez Scaleway (France).
- Surveillance des services chaque minute (status.cdesp.app) avec alerte immédiate en cas de panne.
- Procédure de restauration documentée et testée.

### Minimisation

- Mesure d'audience uniquement après consentement, champs de saisie masqués dans les enregistrements de session, aucune donnée personnelle dans les événements d'analyse.
- Lecture des plaques signalétiques par des modèles hébergés dans l'Union européenne, sans conservation des images par le prestataire.
- Assistant hébergé en France, sans conservation des questions par le prestataire et sans entraînement de modèles sur les Données Client.

### Organisation

- Liste publique et à jour des Sous-traitants ultérieurs et registre des contrats associés.
- Tests automatisés et vérification sur l'environnement de test avant chaque mise en production.
- Procédure de gestion des Violations de données conforme à l'article 11.

## Annexe C. Sous-traitants ultérieurs autorisés

Liste à la date du présent accord ; mises à jour selon l'article 8 et sur cdesp.app/sous-traitants.

| Prestataire | Mission | Lieu du traitement | Garantie en cas de transfert |
|---|---|---|---|
| MXSoft LLC (États-Unis) | Développement, hébergement, maintenance, support technique et exploitation de la Plateforme | Données dans l'Union européenne ; accès d'administration depuis les États-Unis | Clauses contractuelles types (accord de traitement entre DCRR et MXSoft LLC) |
| Hetzner Online GmbH (Allemagne) | Serveurs de l'application, de la base de données, de la messagerie et de la base documentaire de l'assistant | Allemagne (Nuremberg) | Aucun transfert |
| Scaleway SAS (France) | Copie de secours quotidienne chiffrée de la base | France | Aucun transfert |
| Cloudflare Inc. | Réseau, anti-robot, stockage des fichiers et des sauvegardes, mises à jour de l'application mobile | Fichiers et sauvegardes dans l'Union européenne ; réseau mondial | Cadre de protection des données UE-États-Unis et clauses contractuelles types |
| Mistral AI SAS (France) | Assistant cDESP : réponses aux questions et recherche dans les documents | France | Aucun transfert |
| OpenRouter Inc. | Lecture automatique des plaques signalétiques | Union européenne (modèles hébergés dans l'UE, sans conservation) | Traitement dans l'Union européenne |
| Resend Inc. | Envoi des e-mails déclenchés par le Client (rendez-vous, demandes de signature, rappels d'échéances) | États-Unis | Cadre de protection des données UE-États-Unis ou clauses contractuelles types (à confirmer) |
| PostHog Inc. | Mesure d'audience et enregistrement des sessions après consentement de l'Utilisateur, champs de saisie masqués | Allemagne (Francfort) | Clauses contractuelles types |
| Google (Firebase) | Notifications de l'application Android | Union européenne et États-Unis | Cadre de protection des données UE-États-Unis et clauses contractuelles types |
| Apple | Notifications de l'application iPhone | États-Unis | Cadre de protection des données UE-États-Unis et clauses contractuelles types |

Stripe (paiements) n'est pas un Sous-traitant ultérieur pour les Données Client : il ne traite que les données de facturation du Client, dont DCRR est responsable de traitement.