

# Accord de sous-traitance RGPD (DPA) - Modele ROOMCA

Article 28 RGPD - Ref. DOC-DPA-01 - les champs {{...}} sont completes a la signature

**Checklist à compléter avant envoi a un client** (champs {{...}} ci-dessous) :

- {{NOM\_EMPLOYEUR}} : raison sociale du Responsable de traitement
- {{ADRESSE\_EMPLOYEUR}} : siège social
- {{SIREN\_EMPLOYEUR}} : numéro RCS / SIREN du Responsable
- {{NOM\_REPRESENTANT}} , {{FONCTION}} : signataire côté client
- {{EMAIL\_DPO\_CLIENT}} : adresse du DPO ou du contact RGPD client
- {{NB\_SALARIES}} : nombre de salariés couverts
- {{DATE PRISE EFFET}} : date d'effet du DPA
- {{VILLE JURIDICTION}} : juridiction compétente (par défaut Lyon)
- {{VILLE SIGNATURE}} , {{DATE SIGNATURE}} : lieu et date a la signature
- {{NB\_EXEMPLAIRES}} : nombre d'exemplaires originaux (défaut 2)

Les informations ROOMCA (article 1) sont déjà pre-remplies pour la SAS ROOMCA (RCS Lyon 105 485 114, SIRET 105 485 114 00018). L'article 16 documente la continuité juridique avec l'Entrepreneur Individuel antérieur pour les clients éventuels signés avant le 28/05/2026.

## Accord de sous-traitance des données a caractère personnel (DPA) - ROOMCA /

### {{NOM\_EMPLOYEUR}}

*Établi en application de l'article 28 du Règlement Général sur la Protection des Données (RGPD, UE 2016/679) et de la loi n. 78-17 du 6 janvier 1978 modifiée. Contrat accessoire au contrat de prestation entre les parties ; en cas de contradiction sur le traitement des données personnelles, le présent accord prévaut.*

**Référence** : DOC-DPA-01 **Version** : 1.4 **Date de version** : 2026-08-17 **Documents associés** (disponibles dans l'espace admin > Légal > Documents) :

- Liste des sous-traitants ultérieurs ROOMCA (réf. DOC-SUBPROC-01)
- AIPD ROOMCA sur les simulations d'hameçonnage (réf. DOC-AIPD-01)
- Charte des simulations (réf. DOC-CHART-01)
- Modèle d'information CSE (réf. DOC-CSE-01)

## Entre

**{{NOM\_EMPLOYEUR}}** (ci-après "le Responsable de traitement"), dont le siège social est situé {{ADRESSE\_EMPLOYEUR}}, immatriculée sous le numéro SIREN {{SIREN\_EMPLOYEUR}}, représenté par {{NOM\_REPRESENTANT}}, agissant en qualité de {{FONCTION}}.

**Et ROOMCA** (ci-après "le Sous-traitant" ou "ROOMCA"), Société par Actions Simplifiée au capital de 1 000 euros, dont le siège social est situé 4 avenue des Frères Lumière, 69008 Lyon (France), immatriculée au Registre du Commerce et des Sociétés de Lyon sous le numéro 105 485 114 (SIRET 105 485 114 00018), assujettie à la TVA (n° de TVA intracommunautaire FR32105485114), représentée par sa Présidente, Madame Lise BENOIT, ayant tous pouvoirs a l'effet des présentes.

ROOMCA est joignable en qualité de point de contact RGPD a l'adresse [contact@roomca.fr](mailto:contact@roomca.fr).

## Article 1 - Objet

Le present accord encadre le traitement de données a caractère personnel par ROOMCA, agissant en qualité de sous-traitant au sens de l'article 4.8 du RGPD, pour le compte du Responsable de traitement, dans le cadre de la fourniture de la plateforme ROOMCA de sensibilisation a la cybersécurité.

La plateforme comprend :

- Des scenarios de sensibilisation par l'expérience (méthode "Cybervécu") accessibles aux salariés du Responsable.
- Des simulations d'hameçonnage (phishing simulation) et de hameçonnage par QR code (quishing) déclenchées a l'initiative du Responsable, encadrées par la charte phishing (réf. DOC-CHARTTE-01).
- Le stockage, l'agrégation et la restitution des resultats pédagogiques.
- Des fonctions d'intégration : SSO OIDC/SAML, webhooks événementiels, API publique de lecture, et notifications ou assistant Roomy via Slack, Microsoft Teams et Google Chat lorsque le Responsable les active.

## Article 2 - Nature, portée et finalité du traitement

- **Nature** : collecte, stockage, analyse agrégée et restitution de données relatives a la vigilance cyber des salariés du Responsable.
- **Portee** : {{NB\_SALARIES}} salariés du Responsable, sur la base d'une information collective préalable.
- **Finalité principale** : exécution par le Responsable de son obligation de sécurité (article 32 RGPD, directive NIS2, référentiels ANSSI).
- **Finalité annexe** : fourniture de tableaux de bord agrégés destinés à la fonction RSSI/DSI du Responsable.
- **Finalités exclues** : evaluation individuelle des salariés au sens des articles L.1222-2 et suivants du Code du travail, identification nominative dans les reportings publics, prospection commerciale.
- **Durée** : durée du contrat de prestation entre ROOMCA et le Responsable, prorogée des délais de conservation prévus à l'article 11.

**Recours a l'intelligence artificielle.** Certaines fonctions de la plateforme (assistant Roomy, aides a la redaction) reposent sur des modeles d'IA generative. L'inference correspondante est operee **en France** (Scaleway Generative APIs, declare dans la liste des sous-traitants ulterieurs). Elle s'exerce dans les limites suivantes, qui constituent un engagement contractuel de ROOMCA :

- **Donnees transmises au modele**, selon la fonction : l'assistant administrateur et les canaux Slack ou Teams ne transmettent aucun contexte individuel ; le coach apprenant et le message hebdomadaire de suivi transmettent le **prenom** de la personne et son **contexte de progression** (niveau, serie en cours, nombre de scenarios joues, score moyen, axe de reflexe le plus faible), afin de personnaliser la reponse. Ni nom de famille, ni adresse e-mail, ni contenu de simulation.
- Les contenus soumis **ne sont pas reutilises** pour entrainer des modeles.
- **Aucune decision automatisee** au sens de l'article 22 du RGPD n'est produite : les sorties sont des propositions soumises a la relecture d'un utilisateur.
- Les scenarios du catalogue sont fabriques par ROOMCA **en amont** du service, hors traitement de donnees du Responsable (voir la liste des sous-traitants ulterieurs).

Cette information est destinee a etre reportee au registre des traitements du Responsable lorsqu'il active ces fonctions.

## Article 3 - Catégories de personnes concernées et de données

**Personnes concernées** : les salariés du Responsable inscrits a la plateforme, ainsi que tout autre collaborateur (stagiaire, alternant, prestataire) que le Responsable choisit d'inscrire.

**Données traitees** :

| Catégorie             | Exemple                                                                            | Source                                                     |
|-----------------------|------------------------------------------------------------------------------------|------------------------------------------------------------|
| Identification        | Nom, prenom, email professionnel                                                   | RH du Responsable, ou import CSV, ou auto-provisioning SSO |
| Organisation          | Departement, poste, responsable hierarchique (optionnel)                           | Responsable                                                |
| Activite pedagogique  | Horodatages d'ouverture, clic, signalement, scores par scenario, badges            | Plateforme                                                 |
| Comportement campagne | Horodatages d'ouverture et de clic sur emails de simulation                        | Pixel + URL signee                                         |
| Technique             | Adresse IP collectee puis anonymisee, user-agent tronque (browser + OS uniquement) | Serveur                                                    |
| Authentification      | Hash du mot de passe (Argon2id), secret MFA chiffre, jetons de session             | Plateforme                                                 |
| Logs                  | Logs d'audit horodates des actions administratives                                 | Plateforme                                                 |

**Pas de données sensibles au sens de l'article 9 RGPD** (sante, opinions, origine, orientation, biometrie, données genetiques) ni de **données relatives a des condamnations** (article 10) ni de **NIR**.

**Pas de stockage des réponses saisies dans les formulaires pièges** : les credentials soumis pendant une simulation sont détruits sans être conservés.

#### Article 4 - Instructions documentees du Responsable

ROOMCA traite les données uniquement sur instruction documentee du Responsable. Constituent des instructions documentees :

1. La configuration de la plateforme par les comptes administrateurs désignés du Responsable.
2. Les paramètres de retention configurés par le Responsable.
3. Tout courrier électronique adressé à `contact@roomca.fr` par un signataire ou un administrateur désigné.
4. Le cas échéant, les obligations légales auxquelles ROOMCA est tenu (auquel cas ROOMCA en informe le Responsable, sauf interdiction légale).

Si une instruction paraît constituer une violation du RGPD, ROOMCA en informe immédiatement le Responsable.

#### Article 5 - Obligations du Sous-traitant (ROOMCA)

ROOMCA s'engage a :

1. **Traiter les données uniquement** pour les finalités de l'article 2 et sur les instructions de l'article 4.
2. Garantir la **confidentialité** des personnes habilitées a traiter les données : Lise BENOIT (Présidente) et Matis SONZINI (Directeur general) sont les seules personnes autorisées a accéder aux données client en production, tenues a une obligation de confidentialité, et utilisant un accès administratif protégé par MFA et par tunnel VPN (WireGuard) fermé depuis l'Internet public.
3. Mettre en oeuvre les **mesures techniques et organisationnelles (MTO)** décrites en Annexe 1, conformes a l'article 32 RGPD.
4. **Ne pas faire appel a un autre sous-traitant** sans accord écrit préalable du Responsable. La liste a jour des sous-traitants ultérieurs autorises figure dans la Liste des sous-traitants ROOMCA (réf. DOC-SUBPROC-01), intégrée au présent accord par renvoi.
5. **Tenir un registre** des catégories d'activites de traitement effectuées pour le compte du Responsable (article 30.2 RGPD).
6. Assister le Responsable, compte tenu de la nature du traitement et des informations disponibles, pour :
  - Répondre aux demandes d'exercice des droits des personnes concernées (articles 12 a 23 RGPD).
  - Réaliser les analyses d'impact (AIPD, article 35), en mettant a disposition l'AIPD pre-faite ROOMCA (réf. DOC-AIPD-01).
  - Consulter préalablement l'autorité de contrôle si requis (article 36).
  - Garantir la sécurité des données (article 32) et la notification de violation (articles 33-34).
7. **À l'issue du contrat**, restituer ou detruire l'ensemble des données personnelles selon le choix du Responsable, dans les conditions de l'article 12.
8. **Mettre a disposition** toute information nécessaire pour démontrer le respect des obligations du présent accord et permettre la réalisation d'audits dans les conditions de l'article 10.

## Article 6 - Obligations du Responsable de traitement

Le Responsable s'engage a :

1. **Informers les salariés** conformément aux articles 13 et 14 RGPD : charte IT, note d'information dédiée, information du CSE préalable au sens de l'article L.2312-38 du Code du travail (préavis 15 jours).
2. **Recueillir** le cas échéant les consentements ou la base légale requis.
3. **Tenir le registre des traitements** pour la part le concernant (article 30.1 RGPD).
4. **Documenter ses instructions** a ROOMCA.
5. **Ne pas utiliser** les données individuelles ROOMCA pour évaluer la performance des salariés au sens du droit du travail ni prononcer une sanction disciplinaire.
6. **Désigner** au moins un administrateur du compte ROOMCA et **maintenir à jour la liste** des comptes administrateurs.
7. **Notifier sans délai** a ROOMCA toute réclamation, demande d'exercice de droit ou enquête d'autorité de contrôle concernant le traitement.

## Article 7 - Sous-traitance ultérieure

ROOMCA a une autorisation générale du Responsable pour faire appel aux sous-traitants ultérieurs listés dans la Liste des sous-traitants ROOMCA (réf. DOC-SUBPROC-01). Pour tout ajout ou remplacement significatif :

- **Notification** par email au Responsable au moins **30 jours avant** la mise en oeuvre.
- **Droit d'opposition** : le Responsable peut s'opposer par retour écrit dans ce délai. Si l'opposition rend l'exécution du contrat impossible, le Responsable peut résilier sans pénalité, avec restitution des données sous 30 jours.
- **Garanties** : ROOMCA impose contractuellement a chaque sous-traitant ultérieur des obligations équivalentes a celles du présent accord (article 28.4 RGPD), notamment l'interdiction de transfert hors UE sans garanties appropriées.

## Article 8 - Droits des personnes concernées

ROOMCA assiste le Responsable dans le traitement des demandes d'exercice de droits. Les fonctionnalités suivantes sont disponibles :

| Droit                   | Modalité                                                                                           |
|-------------------------|----------------------------------------------------------------------------------------------------|
| Accès (art. 15)         | Export JSON ou CSV sur demande, dans un délai de 30 jours                                          |
| Rectification (art. 16) | Self-service dans le compte apprenant ou via admin                                                 |
| Effacement (art. 17)    | Suppression sous 30 jours, neutralisation des clés étrangères préservant l'intégrité référentielle |
| Limitation (art. 18)    | Désactivation du compte, conservation sans usage                                                   |
| Opposition (art. 21)    | Demande écrite au point de contact, retrait sous 15 jours, sans justification                      |
| Portabilité (art. 20)   | Export JSON structure sur demande                                                                  |

Le délai de réponse cumule (ROOMCA + Responsable) ne peut excéder un mois, sauf prolongation justifiée (article 12.3 RGPD).

## Article 9 - Notification de violation de données

En cas de violation au sens de l'article 4.12 RGPD :

- **Délai** : notification au Responsable **sous 24 heures** après détection, par email au {{EMAIL\_DPO\_CLIENT}}.
- **Contenu** : nature de la violation, catégories et nombre approximatif de personnes concernées, catégories et nombre approximatif d'enregistrements, conséquences probables, mesures prises ou envisagées pour y remédier et en atténuer les effets.
- **Assistance** : ROOMCA assiste le Responsable dans la notification a la CNIL (article 33) et, le cas échéant, aux personnes concernées (article 34), en lui fournissant toute information utile.
- **Documentation** : ROOMCA tient un registre interne des violations comme prévu a l'article 33.5 RGPD.

## Article 10 - Audit et contrôle

Le Responsable dispose d'un **droit d'audit** documentaire sur les obligations du présent accord. ROOMCA met a disposition, dans un délai de 30 jours après demande écrite :

1. La dernière version de la description des mesures techniques et organisationnelles (Annexe 1).
2. La liste à jour des sous-traitants ultérieurs et leurs certifications.
3. Les rapports d'audit interne disponibles, le cas échéant.
4. L'AIPD ROOMCA (réf. DOC-AIPD-01).

Un **audit sur site ou à distance** par le Responsable ou un auditeur mandate (tiers indépendant soumis au secret professionnel, accepté par ROOMCA) peut être demandé, dans les conditions suivantes :

- Préavis écrit de **60 jours minimum**.
- Fréquence maximale d'**une fois par an**, sauf en cas de violation avérée ou de demande motivée d'une autorité de contrôle.
- Plage horaire raisonnable, sans perturbation déraisonnable de l'activité de ROOMCA.
- Périmètre limité aux données du Responsable et aux moyens déployés pour leur traitement.
- Coûts de l'audit à la charge du Responsable, sauf si l'audit révèle un manquement significatif de ROOMCA, auquel cas les coûts sont à la charge de ROOMCA.

ROOMCA peut, en alternative et sous réserve d'acceptation expresse du Responsable, fournir un rapport d'audit indépendant (type SOC 2 ou ISO 27001 lorsqu'il aura été réalisé) couvrant le périmètre audité.

## Article 11 - Durée de conservation des données

Sauf instruction contraire du Responsable :

| Données                                                              | Durée                                                                                    |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Identification et activité pédagogique                               | 24 mois après le dernier exercice de l'utilisateur                                       |
| Scores et historique des scénarios                                   | 36 mois après le dernier exercice                                                        |
| Logs d'audit et de sécurité                                          | 12 mois (365 jours, purge automatique quotidienne, paramétrable par contrat)             |
| Données techniques (scans QR, pairings)                              | 180 jours / 90 jours / 30 jours selon catégorie (conformément aux durées minimales RGPD) |
| Sauvegardes (journaux de transaction, base physique, export logique) | 30 jours roulants                                                                        |

À la résiliation du contrat de prestation, l'ensemble des données est supprimé ou restitué selon l'article 12, indépendamment des durées ci-dessus.

## Article 12 - Réversibilité et fin de contrat

À l'issue du contrat de prestation, quelle qu'en soit la cause, ROOMCA s'engage à :

1. **Sur demande écrite du Responsable formulée dans les 30 jours suivant la fin du contrat** :
  - **Restituer** l'ensemble des données personnelles dans un format structuré : export JSON ou CSV chiffré (mot de passe transmis sur un canal distinct), transmis via lien HTTPS signé (validité 7 jours) ou support physique chiffré selon le volume.
  - Inclure un fichier `schema.json` décrivant la structure des données exportées.
2. **Détruire** l'ensemble des données originelles et leurs copies dans un délai de **30 jours** après restitution (ou après la fin du contrat si aucune restitution n'est demandée), y compris les sauvegardes qui expirent par rotation naturelle dans le délai de 30 jours.
3. **Fournir un bordereau de destruction** signé par Lise BENOIT, attestant de la destruction effective (modèle en Annexe 2).
4. **Conserver uniquement** les données pour lesquelles ROOMCA est légalement tenu (factures comptables : 10 ans ; logs de sécurité spécifiques : selon obligation légale).

## Article 13 - Transferts de données hors Union européenne

ROOMCA n'héberge **aucune donnée personnelle hors de l'Union européenne**.

L'ensemble des données est hébergé en France (Scaleway PAR1). Les seuls flux extérieurs à l'UE sont limitativement énumérés ci-dessous :

- **Let's Encrypt (ISRG)** : transfert du nom de domaine `roomca.fr` (donnée publique) pour l'émission de certificats TLS automatisés. Ce flux n'est pas un transfert de données personnelles au sens du RGPD.
- **Infomaniak** : réception des emails entrants `@roomca.fr` (boîte éditeur, sans donnée client), hébergé en Suisse, bénéficiant d'une décision d'adéquation de la Commission européenne.
- **Google Safe Browsing** (États-Unis) : vérification de la réputation d'une URL par les fonctions de vigilance mail et d'analyse de liens. **Seule l'adresse du lien est transmise** : aucune identité, aucun contenu de message, aucune donnée d'apprenant. Flux encadré par le Data Privacy Framework UE-US et des clauses contractuelles types.

Aucun autre transfert n'est réalisé. La mesure d'audience Google Analytics porte exclusivement sur les pages marketing publiques de `roomca.fr`, pour lesquelles ROOMCA est responsable de traitement : elle est hors du périmètre du présent accord et ne traite aucune donnée d'apprenant. Si ROOMCA envisageait un transfert hors UE, il en informerait préalablement le Responsable et obtiendrait son accord écrit, et mettrait en place les garanties appropriées au titre des articles 44 à 49 RGPD.

## Article 14 - Responsabilité et indemnisation

ROOMCA et le Responsable rependent chacun de leurs manquements respectifs aux obligations du RGPD et du présent accord.

**Plafond de responsabilité contractuelle de ROOMCA** au titre du présent accord, tous préjudices confondus et toutes causes confondues sur une période de 12 mois glissants : **montant des sommes effectivement payées par le Responsable à ROOMCA au titre du contrat de prestation au cours des 12 mois précédant le fait générateur.**

Ce plafond ne s'applique pas en cas de faute lourde, de dol, ou de violation délibérément causée par ROOMCA. Il ne s'applique pas non plus aux sanctions administratives prononcées à l'encontre du Responsable du fait d'un manquement avéré de ROOMCA, qui restent dues intégralement.

## Article 15 - Continuité d'activité et plan de reprise

ROOMCA met en œuvre :

- **Sauvegarde continue de la base de données applicative PostgreSQL** : archivage des journaux de transaction (`archive_timeout` de 60 secondes) expédiés chaque minute vers Scaleway Object Storage PAR1, base physique quotidienne servant de point de départ à une restauration à un instant précis (PITR), export logique horaire en fichier. Tous **chiffres GPG AES-256 avant tout départ du serveur. RPO inférieur à 1 minute.**
- **Procédure de restauration documentée et testée de bout en bout** sur les deux chemins (export logique et PITR), avec re-test périodique. Un sinistre réel a été traité le 2026-07-21 : perte du volume de la VM de production, reconstruite depuis les sauvegardes.
- **RTO cible** : 4 heures en cas d'incident majeur (perte de la VM principale).
- **Tunnel d'administration WireGuard** maintenu pour l'intervention d'urgence.
- **Monitoring d'erreur** via GlitchTip auto-hébergé (alertes 5xx avec scrubbing PII).

En cas d'indisponibilité prolongée (supérieure à 72 heures), ROOMCA en informe le Responsable et fournit un plan de rétablissement.

## Article 16 - Continuité juridique

ROOMCA est une Société par Actions Simplifiée constituée le 28 mai 2026 (RCS Lyon 105 485 114, SIRET 105 485 114 00018, capital 1 000 euros), qui exerce désormais l'activité anciennement exploitée par Madame BENOIT Lise Charlotte sous le statut d'Entrepreneur Individuel (ancien SIRET 932 287 634 00020).

Pour les clients ayant signé un DPA avec l'Entrepreneur Individuel antérieur, ROOMCA SAS reprend de plein droit l'intégralité des engagements souscrits, sans interruption du service ni nouvelle signature requise. Un avenant de substitution peut être fourni sur demande écrite à [contact@roomca.fr](mailto:contact@roomca.fr), mentionnant la dénomination sociale, le SIRET, le RCS, le siège social de la SAS et la date d'effet de la substitution (28 mai 2026).

Les données ne font l'objet d'aucun transfert à un nouveau sous-traitant : elles restent sous la responsabilité des mêmes personnes physiques (Lise BENOIT et Matis SONZINI), désormais dirigeants de la SAS.

## Article 17 - Mises à jour du présent accord

Le présent accord peut être amendé :

- À la demande de l'une des parties pour se conformer à une évolution légale ou réglementaire.

- Suite a la publication d'une version mise a jour de la liste des sous-traitants ultérieurs (article 7).
- Suite a une evolution significative des MTO (Annexe 1) ou des durées de conservation (article 11).

Toute mise a jour est notifiée par email au Responsable. En l'absence d'opposition motivée dans un délai de 30 jours, la nouvelle version est réputée acceptée.

Article 18 - Droit applicable et juridiction

Le present accord est soumis au **droit francais** et aux dispositions du RGPD directement applicables.

A défaut de resolution amiable dans un délai de 60 jours, tout litige relatif au présent accord est de la competence exclusive des tribunaux de **{{VILLE\_JURIDICITION}}**.

Fait en **{{NB\_EXEMPLAIRES}}** exemplaires originaux, a **{{VILLE\_SIGNATURE}}**, le **{{DATE\_SIGNATURE}}**.

Le present accord peut etre signe **electroniquement** via le service de signature integre ROOMCA (verification d'identite par code a usage unique, horodatage qualifié et journal de preuve scelle), reconnu entre les parties au sens du reglement eIDAS (UE n. 910/2014) et des articles 1366 et 1367 du Code civil. ROOMCA y appose ensuite son sceau electronique. La signature electronique a la meme valeur probante qu'une signature manuscrite ; un exemplaire papier signe de maniere manuscrite reste admis.

| Pour le Responsable de traitement                   | Pour ROOMCA (Sous-traitant)                              |
|-----------------------------------------------------|----------------------------------------------------------|
| <b>{{NOM_REPRESENTANT}}</b>                         | <b>Lise BENOIT</b>                                       |
| <b>{{FONCTION}}</b>                                 | Présidente de ROOMCA SAS                                 |
| <b>{{NOM_EMPLOYEUR}}, SIREN {{SIREN_EMPLOYEUR}}</b> | SIRET 105 485 114 00018, RCS Lyon                        |
|                                                     | <a href="mailto:contact@roomca.fr">contact@roomca.fr</a> |
| Signature et cachet :                               | Signature :                                              |
|                                                     |                                                          |
|                                                     |                                                          |
|                                                     |                                                          |

Annexe 1 - Mesures techniques et organisationnelles (MTO)

Mesures en vigueur à la date de signature, susceptibles d'évolution conformément à l'article 17.

1.1 Hébergement et chiffrement

- Hébergement applicatif et base de données sur **Scaleway PAR1** (Paris, France), prestataire certifié ISO 27001:2022 et HDS (juillet 2024).
- **Chiffrement en transit** : TLS 1.3 avec suite hybride post-quantique X25519MLKEM768 activée via Caddy (vérifié par test client Go au déploiement du certificat).
- **Chiffrement au repos des secrets et données sensibles** : AES-256-GCM applicatif sur les jetons et secrets stockés.
- **Sauvegardes chiffrées** : chiffrement GPG AES-256 appliqué sur le serveur avant tout envoi, puis SSE-AES256 côté Scaleway Object Storage. Archivage continu des journaux de transaction PostgreSQL expédiés chaque minute (RPO inférieur à 1 minute), base physique quotidienne, export logique horaire. Rétenion : 30 bases physiques, 35 jours de journaux, 30 jours d'exports logiques.

1.2 Authentification et contrôle d'accès

- **Authentification utilisateurs** : mot de passe long (12 caractères minimum), hash Argon2id, vérification de robustesse en temps réel.
- **MFA** : obligatoire pour les comptes ROOMCA disposant d'un accès d'administration, activable en obligation à l'échelle d'une société cliente par le réglage `mfa_required` (relayé au fournisseur d'identité en cas de SSO), optionnel pour les apprenants sinon, supporte TOTP (Microsoft Authenticator, Google Authenticator, etc.) avec codes de récupération.
- **SSO** : OIDC (Azure AD, Google Workspace, Okta) et SAML 2.0 self-service par tenant, avec scoping strict `company_id` pour prévenir l'usurpation inter-tenant.
- **Rôles (RBAC)** : `super_admin`, `admin`, `group_admin`, `player`. Scope `company_id` vérifié à chaque requête protégée.
- **Sessions** : refresh tokens HttpOnly signés, timeout d'inactivité par rôle (1h `super_admin`, 2h autres).

- **Accès administrateur ROOMCA** : SSH fermé sur Internet public, accès unique via tunnel WireGuard, clé SSH personnelle, journalisation système.

### 1.3 Sécurité applicative

- **Protection brute-force** : verrouillage progressif après 5 échecs de login, anti-énumération sur l'endpoint forgot-password.
- **Rate limiting** : par adresse IP et par utilisateur sur les endpoints sensibles (auth, MFA, écriture, soumission de résultats).
- **CSRF** : tokens double-submit sur toutes les requêtes à effet de bord, exemption explicite et justifiée pour les endpoints SAML ACS.
- **Validation des entrées** : schémas Zod sur toutes les routes API, refus systématique des valeurs non conformes.
- **Uploads** : vérification par magic bytes + whitelist MIME stricte, refus des SVG, limitation de taille.
- **Protection IDOR** : vérification du scope company\_id sur chaque accès ressource.
- **Headers de sécurité** : CSP stricte avec report-only en parallèle, HSTS, X-Content-Type-Options, COOP, CORP, X-Frame-Options DENY.

### 1.4 Monitoring et journalisation

- **GlitchTip auto-hébergé** : monitoring des erreurs 5xx applicatives, scrubbing PII actif (emails, IPs, identifiants).
- **CrowdSec** : détection des comportements abusifs (scan, brute-force, scrapping) avec banissement IP.
- **Audit logs horodatés** des actions administratives, conservés 24 mois.
- **Détection PII dans les logs** : filtres automatiques avant tout export.

### 1.5 Sécurité opérationnelle

- **Mises à jour de sécurité** : application sous 72 heures pour les CVE critiques affectant le runtime (Node.js, Caddy, OpenSSL, lib applicatives), sous 30 jours pour les autres.
- **Surveillance vulnérabilités** : suivi des avis CERT-FR, ANSSI, GitHub Advisory Database via flux intégré dans le tableau de bord ROOMCA.
- **Veille fuites email** : abonnement au service XposedOrNot, alerte automatique si un email salarié apparaît dans une fuite publique (notification à l'admin client uniquement, jamais de divulgation publique).
- **Pas de tests d'intrusion tiers actuels** : un audit indépendant sera planifié au cours des 12 mois suivant la signature du premier contrat entreprise. Le rapport synthétique sera mis à disposition sur demande sous accord de confidentialité.

### 1.6 Organisation et personnel

- **Personnel autorisé** : Lise BENOIT (Présidente) et Matis SONZINI (Directeur général), signataires du présent accord, seules personnes ayant accès à l'infrastructure de production.
- **Engagement de confidentialité** : les dirigeants de ROOMCA SAS sont tenus contractuellement à une obligation de discrétion absolue sur toutes les données client traitées, conformément à l'article 28.3.b RGPD.
- **Coopération avec un futur collaborateur** : tout salarié ou prestataire ultérieur signera un engagement de confidentialité écrit conforme à l'article 28.3.b RGPD avant tout accès aux données de production. La liste des personnes autorisées sera tenue à jour et fournie sur demande.
- **Formation** : ROOMCA documente en interne ses propres scénarios de sensibilisation cyber et les applique à ses opérations (eat-your-own-dog-food).

### 1.7 Conformité documentaire

ROOMCA maintient une documentation interne de mapping de ses contrôles vers les référentiels suivants :

- **RGPD** (UE 2016/679 + loi 78-17)
- **NIS2** (directive UE 2022/2555)
- **DORA** (règlement UE 2022/2554, en tant que prestataire de services TIC pour le secteur financier)
- **HDS** (héritage du cadre Scaleway, applicable à des extensions futures)
- **ISO 27001** (auto-mapping non certifié à date)
- **ISO 22301** (continuité d'activité, auto-mapping non certifié à date)
- **CRA** (règlement UE 2024/2847 sur la cybersécurité des produits numériques, applicable au plus tard à partir de décembre 2027)
- **ANSSI - Recommandations 42 pour les hébergeurs de données sensibles**

Cette documentation est mise à disposition du Responsable sur demande motivée.

---

## Annexe 2 - Modèle de bordereau de destruction des données

À remettre au Responsable après exécution de la procédure prévue à l'article 12.

### BORDEREAU DE DESTRUCTION DES DONNEES A CARACTERE PERSONNEL

Référence contrat de prestation : \_\_\_\_\_

Référence DPA : DOC-DPA-01, version 1.4, signé le \_\_\_\_\_

Responsable de traitement : \_\_\_\_\_

Sous-traitant : ROOMCA SAS, SIRET 105 485 114 00018, RCS Lyon,  
4 avenue des Frères Lumière, 69008 Lyon (France)

Je soussignée, Lise BENOIT, Présidente de ROOMCA SAS, atteste que :

1. L'ensemble des données personnelles traitées pour le compte du Responsable précité a été supprimé de l'environnement de production de ROOMCA le \_\_\_\_\_.
2. Les sauvegardes résiduelles contenant ces données expirent par rotation naturelle au plus tard le \_\_\_\_\_ (date + 30 jours après suppression de production).
3. Aucune copie n'est conservée dans les environnements de développement, de test, ou sur des supports amovibles.
4. Les données pour lesquelles ROOMCA est légalement tenu de conserver (factures comptables principalement) sont les suivantes :  
\_\_\_\_\_

Si une restitution préalable a été effectuée, elle a été réalisée :

- Date : \_\_\_\_\_
- Format : \_\_\_\_\_ (JSON / CSV / autre)
- Canal : \_\_\_\_\_ (HTTPS signé / support chiffré / autre)
- Volume : \_\_\_\_\_

Fait à Lyon, le \_\_\_\_\_.

Signature : Lise BENOIT

## Annexe 3 - Coordonnées et points de contact

| Sujet                                                   | Contact ROOMCA                                                                                                         |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Question generale RGPD                                  | <a href="mailto:contact@roomca.fr">contact@roomca.fr</a>                                                               |
| Notification de violation par le Responsable a ROOMCA   | <a href="mailto:contact@roomca.fr">contact@roomca.fr</a> (mention "[Violation RGPD]" en sujet, traitement prioritaire) |
| Demande d'audit                                         | <a href="mailto:contact@roomca.fr">contact@roomca.fr</a> (mention "[Audit DPA]" en sujet)                              |
| Demande d'exercice de droits par une personne concernee | <a href="mailto:contact@roomca.fr">contact@roomca.fr</a> (mention "[Demande RGPD]" en sujet)                           |
| Demande de bordereau de destruction                     | <a href="mailto:contact@roomca.fr">contact@roomca.fr</a>                                                               |

ROOMCA s'engage a accuser réception sous **48 heures ouvrées** et a apporter une reponse circonstanciée sous **15 jours ouvrés** maximum.

Fin du document.

