Politique de Confidentialité

1. Identité du responsable de traitement

La présente Politique de Confidentialité décrit la manière dont :

RociaDB
Forme juridique : SAS
Capital social : 1000€
Siège social : 20 PLACE EDMOND CANET 81000 ALBI
SIREN/SIRET : 104 716 360 / 104 716 360 00011
Email de contact : legal@rociadb.com
(Ci-après « l'Éditeur », « nous », « notre société »)
Traite les données à caractère personnel dans le cadre :

- De l'exploitation de la plateforme SaaS
- De l'utilisation du site internet
- De la gestion des comptes clients
- Des échanges commerciaux et contractuels
- Des services techniques proposés via APIs et SDK

2. Champ d'application

La présente politique s'applique :

- Aux visiteurs du site internet
- Aux prospects
- Aux clients professionnels & Particulier
- Aux utilisateurs de la plateforme SaaS
- Aux utilisateurs des APIs et SDK
- Aux personnes contactant notre support

3. Rôles RGPD

3.1 Données des clients hébergées via la plateforme

Dans le cadre des données stockées par les clients via la plateforme SaaS, l'Éditeur agit exclusivement en qualité de sous-traitant au sens du RGPD.
Les clients demeurent seuls responsables :

- Des finalités des traitements
- Des données importées
- Des obligations d'information
- Des bases légales
- Des durées de conservation

L'Éditeur n'exploite pas les données hébergées à des fins propres.

3.2 Données traitées directement par l'Éditeur

L'Éditeur agit en qualité de responsable de traitement pour les traitements liés notamment :

- À la création des comptes clients
- À l'authentification
- À la gestion administrative
- À la facturation
- À la sécurité
- Au support technique
- À la gestion contractuelle
- Au respect des obligations légales

4. Données collectées

Les données susceptibles d'être collectées comprennent notamment :

Données d'identification

- Nom
- Prénom
- Société
- Adresse email
- Adresse Postale
- Numéro de téléphone
- Identifiant utilisateur

Données techniques

- Adresse IP
- Logs techniques
- Tenant id
- Request_id
- Métadonnées techniques
- Journaux d'accès
- Informations de sécurité
- Données d'authentification
- Compte de service OIDC

Données liées à l'utilisation de la plateforme

- Documents JSON
- Fichiers binaires
- Graphes
- Métadonnées fichiers
- Informations de configuration

Données contractuelles et administratives

- Informations de facturation
- Historique des abonnements
- Échanges support

5. Finalités des traitements

Gestion des comptes et fourniture des services

Création et gestion des comptes

Le traitement des données est fondé sur l'exécution du contrat conclu avec l'utilisateur.

Fourniture de la plateforme SaaS

Le traitement est nécessaire à l'exécution contractuelle afin de permettre l'accès et l'utilisation des services proposés par la plateforme.

Gestion du support

Les données traitées dans le cadre du support client reposent sur l'exécution contractuelle afin d'assurer l'assistance et le suivi des demandes utilisateurs.

Sécurité et fonctionnement technique

Authentification et sécurité

Le traitement repose sur l'intérêt légitime de l'organisme afin de garantir la sécurité des comptes, des accès et des systèmes d'information.

Prévention des incidents et sécurité

Les traitements mis en œuvre pour détecter, prévenir et gérer les incidents de sécurité sont fondés sur l'intérêt légitime de l'organisme.

Journalisation technique

Les journaux techniques et logs de connexion sont traités sur la base de l'intérêt légitime afin d'assurer la traçabilité, la sécurité et le bon fonctionnement de la plateforme.

Obligations administratives et réglementaires

Facturation et comptabilité

Les traitements liés à la facturation et à la comptabilité reposent sur une obligation légale applicable à l'organisme.

Respect des obligations réglementaires

Les traitements nécessaires au respect des obligations réglementaires et légales reposent sur l'obligation légale.

Communication et prospection commerciale

Prospection commerciale B2B

Les actions de prospection commerciale à destination des professionnels reposent sur l'intérêt légitime de l'organisme.

Newsletter marketing

L'envoi de newsletters et communications marketing repose sur le consentement de la personne concernée lorsque celui-ci est requis par la réglementation applicable.

6. Cookies et traceurs

6.1 Cookies techniques

Le site et la plateforme utilisent des cookies strictement nécessaires au fonctionnement du service.

Ces cookies ne nécessitent pas de consentement préalable.

6.2 Cookies de mesure d'audience et autres traceurs :

Aucun cookies de mesure d'audience est de traceurs n'est utilisés

7. Destinataires des données

Les données peuvent être accessibles :

- Aux équipes habilitées
- Aux prestataires techniques
- Aux hébergeurs
- Aux sous-traitants techniques
- Aux autorités légalement habilitées

8. Sous-traitants

Dans le cadre de la fourniture de ses services, RociaDB peut recourir à des sous-traitants techniques et opérationnels, notamment pour l'hébergement de l'infrastructure, les services cloud, les sauvegardes, la sécurité ou les services de paiement.

À la date de mise à jour de la présente politique, les principaux sous-traitants utilisés par RociaDB sont :

Sous-traitant	Localisation	Nature de la prestation
OVH SAS, opérant sous la marque OVHcloud	Union européenne	Hébergement de l'infrastructure technique, services cloud, stockage, sauvegardes, sécurité et exploitation technique des services RociaDB.
Stripe Payments Europe, Ltd.	Union européenne	Services de paiement, traitement des transactions et opérations associées à la gestion des paiements.

RociaDB s'assure que ses sous-traitants présentent des garanties suffisantes en matière de sécurité, de confidentialité et de conformité au RGPD.

La liste détaillée et à jour des sous-traitants est disponible sur la page « Sous-traitants » du site rociadb.com.

9. Hébergement et transferts de données

Les données liées à l'utilisation de la Solution RociaDB sont hébergées au sein de l'Union européenne par OVH SAS, opérant sous la marque OVHcloud.

RociaDB ne prévoit pas de transfert des données hébergées dans la Solution en dehors de l'Union européenne dans le cadre de son hébergement principal.

Certains services accessoires, notamment les services de paiement fournis par Stripe, peuvent toutefois impliquer des traitements ou transferts de données en dehors de l'Union européenne. Dans ce cas, ces transferts sont encadrés par les garanties appropriées prévues par le RGPD, notamment les clauses contractuelles types ou tout autre mécanisme reconnu par la réglementation applicable.

RociaDB veille à ce que les traitements réalisés par ses sous-traitants soient encadrés contractuellement et limités aux finalités nécessaires à la fourniture des services concernés.

10. Durées de conservation

Les données sont conservées pendant une durée proportionnée aux finalités poursuivies et conformément aux obligations légales applicables.

Données relatives aux clients et aux contrats

Comptes clients actifs

Les données sont conservées pendant toute la durée de la relation contractuelle

Données liées au compte après résiliation

Les données sont conservées pendant une durée maximale de 3 ans à compter de la fin du contrat, sauf obligation légale contraire.

Données de facturation et comptables

Les données sont conservées pendant 10 ans conformément aux obligations comptables et fiscales.

Contrats et documents contractuels

Les documents sont conservés pendant 5 ans à compter de la fin de la relation contractuelle.

Données techniques et de sécurité

Logs techniques de sécurité

Les journaux techniques sont conservés entre 6 et 12 mois maximum selon les finalités de sécurité poursuivies.

Logs d'administration sensibles

Les journaux d'administration sensibles sont conservés pendant 12 mois maximum.

Sauvegardes techniques

Les sauvegardes sont conservées entre 30 et 90 jours selon la politique de sauvegarde applicable.

Comptes de Service inactives

Les comptes de service inactives doivent être supprimées ou révoquées après une période d'inactivité prolongée.

Support et gestion opérationnelle

Tickets support

Les tickets de support sont conservés pendant 3 ans maximum après leur clôture.

Données liées aux incidents de sécurité

Les données sont conservées jusqu'à la clôture du dossier puis peuvent faire l'objet d'un archivage intermédiaire si nécessaire.

Journaux de violation de données

Les journaux de violation de données sont conservés pendant 5 ans dans le cadre de l'obligation d'accountability prévue par le RGPD.

Prospection commerciale et marketing

Données prospects B2B

Les données sont conservées pendant 3 ans à compter du dernier contact avec le prospect.

Newsletter et prospection commerciale

Les données sont conservées jusqu'au retrait du consentement ou pendant 3 ans sans interaction de la personne concernée.

Données de navigation et cookies

Les cookies et données de navigation sont conservés pendant 13 mois maximum.

Données de mesure d'audience

Les données de mesure d'audience sont conservées pendant 25 mois maximum selon la configuration retenue et les recommandations de la CNIL.

Données hébergées pour le compte des clients

Données stockées sur la plateforme

Les données stockées par les clients sur la plateforme sont conservées conformément aux paramètres et instructions définis par le client agissant en qualité de responsable de traitement.

Exercice des droits RGPD

Données liées aux demandes d'exercice des droits

Les données relatives aux demandes d'exercice des droits des personnes concernées sont conservées entre 1 et 3 ans selon le risque contentieux potentiel.

11. Sécurité

L'Éditeur met en œuvre des mesures techniques et organisationnelles appropriées afin de protéger les données personnelles, notamment :

- Chiffrement des données en transit et au repos
- Séparation logique des environnements clients
- Contrôle des accès
- Journalisation
- Surveillance technique
- Mécanismes de sauvegarde
- Sécurisation des APIs et SDK

12. Logs et données techniques

Des journaux techniques peuvent être générés afin :

- D'assurer la sécurité
- De détecter les incidents
- D'assurer le bon fonctionnement du service
- De superviser la plateforme

Ces journaux peuvent contenir :

- Tenant id
- Request_id
- Informations techniques
- Métriques système

L'accès à ces données est strictement limité aux personnes habilitées.

13. Droits des personnes

Conformément à la réglementation applicable, les personnes concernées disposent :

- D'un droit d'accès
- D'un droit de rectification
- D'un droit d'effacement
- D'un droit à la limitation
- D'un droit d'opposition
- D'un droit à la portabilité

- Du droit de définir des directives relatives au sort de leurs données après leur décès.

Les demandes peuvent être adressées à : rgpd@rociadb.com

14. Réclamation

Les personnes concernées disposent du droit d'introduire une réclamation auprès de la CNIL ou de toute autorité de contrôle compétente.

15. Évolution de la politique

L'Éditeur se réserve le droit de modifier la présente Politique de Confidentialité afin :

- De respecter les évolutions légales
- D'adapter la documentation aux évolutions techniques
- De tenir compte des nouveaux services proposés

Les utilisateurs seront informés en cas de modification substantielle

16. Contact

Pour toute question relative à la protection des données personnelles :

RociaDB

Adresse : 20 PLACE EDMOND CANET 81000 ALBI

Email : rgpd@rociadb.com

DPO / Référent RGPD : Aurélie SANNAC

Contrat de sous-traitance DPA

(Article 28 du Règlement (UE) 2016/679 – RGPD)

ENTRE LES SOUSSIGNÉS

Le Responsable de traitement

Le présent contrat est conclu entre :

Le Client, personne morale ou physique utilisant la plateforme RociaDB dans le cadre de ses activités professionnelles et déterminant les finalités ainsi que les moyens essentiels des traitements de données à caractère personnel réalisés au moyen de cette plateforme,

Ci-après dénommé « le Responsable de traitement »,

Et

Le Sous-traitant

ROCIADB, Société éditrice et exploitante de la plateforme logicielle RociaDB.

ROCIADB fournit une solution logicielle en mode SaaS permettant notamment l'hébergement, le stockage, l'organisation, le traitement et la sécurisation des données confiées par ses clients.

Dans le cadre de ces prestations, RociaDB agit exclusivement en qualité de Sous-traitant au sens des articles 4 et 28 du Règlement (UE) 2016/679.

Ci-après dénommée « le Sous-traitant »,

PRÉAMBULE

Le responsable de traitement utilise la plateforme afin de gérer les traitements de données nécessaires à son activité.

Le responsable de traitement détermine seul :

- Les finalités des traitements
- Les catégories de données traitées
- Les personnes concernées
- Les destinataires des données
- Les durées de conservation
- Les habilitations de ses utilisateurs

RociaDB met exclusivement à disposition une plateforme SaaS ainsi que les prestations techniques nécessaires à son exploitation.

Ces prestations comprennent notamment :

- L'hébergement des infrastructures
- Le stockage des données
- L'administration technique de la plateforme
- Les sauvegardes
- La maintenance corrective
- La maintenance évolutive
- Le support utilisateur
- La supervision
- La sécurisation des traitements

Dans le cadre de ces prestations, RociaDB est amené à traiter des données à caractère personnel pour le compte du responsable de traitement.

Les parties reconnaissent que RociaDB agit exclusivement en qualité de Sous-traitant au sens de l'article 28 du RGPD.
La présente convention constitue le contrat de sous-traitance prévu par l'article 28 du Règlement (UE) 2016/679.

ARTICLE 1 – OBJET

Le présent DPA définit les conditions dans lesquelles le sous-traitant est autorisé à traiter des données à caractère personnel pour le compte du responsable de traitement.
Il précise notamment :

- La nature des traitements confiés
- Les catégories de données concernées
- Les obligations respectives des parties
- Les mesures techniques et organisationnelles mises en œuvre
- Les modalités d'assistance
- Les conditions de recours aux sous-traitants ultérieurs
- Les modalités d'audit
- Les règles applicables en cas de violation de données
- Les conditions de restitution ou de suppression des données

Le présent DPA fait partie intégrante du contrat principal conclu entre les parties. En cas de contradiction entre les deux documents, les dispositions du présent DPA prévalent pour toutes les questions relatives à la protection des données personnelles.

ARTICLE 2 – DÉFINITIONS

Pour les besoins du présent contrat, les termes suivants ont la signification qui leur est donnée ci-après :
Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable, au sens de l'article 4 du RGPD.
Traitement : toute opération ou tout ensemble d'opérations appliquées à des données à caractère personnel, qu'elles soient automatisées ou non.
Responsable de traitement : la personne physique ou morale qui détermine les finalités et les moyens essentiels du traitement.
Sous-traitant : la personne physique ou morale qui traite des données à caractère personnel pour le compte du Responsable de traitement.
Sous-traitant ultérieur : tout prestataire auquel le Sous-traitant confie tout ou partie des traitements réalisés pour le compte du Responsable de traitement.
Violation de données à caractère personnel : toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données personnelles.
Services : l'ensemble des prestations fournies par RociaDB dans le cadre de la plateforme SaaS.

ARTICLE 3 – CHAMP D'APPLICATION

Le présent contrat s'applique à l'ensemble des traitements de données à caractère personnel réalisés par RociaDB pour le compte du responsable de traitement dans le cadre des services.
Il couvre notamment les opérations d'hébergement, de stockage, de maintenance, de sauvegarde, de supervision, de télémaintenance et de support technique.
Il s'applique pendant toute la durée de la relation contractuelle et demeure applicable tant que RociaDB conserve ou traite des données pour le compte du responsable de traitement.

ARTICLE 4 – RÉPARTITION DES RESPONSABILITÉS DES PARTIES

4.1 Principes généraux

Les parties reconnaissent que le responsable de traitement et le sous-traitant exercent des responsabilités distinctes au sens du Règlement (UE) 2016/679.
Le responsable de traitement demeure seul responsable de la conformité des traitements qu'il met en œuvre au moyen de la plateforme RociaDB.
Le sous-traitant intervient exclusivement pour fournir les services techniques définis au contrat et ne détermine ni les finalités ni les moyens essentiels des traitements réalisés par le responsable de traitement.

4.2 Responsabilités du Responsable de traitement

Le responsable de traitement demeure notamment responsable :

- De la détermination des finalités des traitements
- Du choix des bases légales applicables
- De l'information des personnes concernées
- Du respect des principes prévus par le RGPD, notamment ceux de licéité, loyauté, transparence, minimisation, exactitude et limitation de la conservation
- Du choix des données enregistrées dans la plateforme
- De la qualité et de l'exactitude des données
- De la gestion des droits d'accès de ses propres utilisateurs
- De la définition des durées de conservation
- De la gestion des demandes d'exercice des droits des personnes concernées

Le responsable de traitement garantit que les données confiées au sous-traitant sont collectées et traitées conformément à la réglementation applicable.

4.3 Responsabilités du Sous-traitant

ROCIADB est responsable :

- De la mise à disposition de la plateforme SaaS
- De la disponibilité des services conformément aux engagements contractuels
- De la sécurité technique des infrastructures
- De la mise en œuvre des mesures techniques et organisationnelles
- De la gestion des sauvegardes
- De la maintenance corrective et évolutive de la plateforme
- De la gestion des incidents techniques
- De l'assistance apportée au responsable de traitement
- De la notification des violations de données

4.4 Limites de responsabilité du Sous-traitant
Le sous-traitant ne saurait être tenu responsable :
- Des données importées par le responsable de traitement
- De leur exactitude
- De leur licéité
- Des traitements décidés par le responsable de traitement
- Des habilitations attribuées par le responsable de traitement à ses utilisateurs
- Des erreurs commises par les utilisateurs du responsable de traitement

Le sous-traitant ne contrôle pas le contenu des données enregistrées par le responsable de traitement.

4.5 Instructions du Responsable de traitement
Le responsable de traitement reconnaît que toutes les opérations de traitement réalisées par le sous-traitant résultent exclusivement de ses propres instructions.

4.6 Responsabilité conjointe exclue
Les parties reconnaissent expressément que le présent contrat ne crée aucune responsabilité conjointe au sens de l'article 26 du RGPD.
ROCIADB intervient exclusivement en qualité de sous-traitant.
Le client intervient exclusivement en qualité de responsable de traitement.

ARTICLE 5 – OBLIGATIONS DE ROCIADB EN QUALITÉ DE SOUS-traitant
5.1 Principe général
ROCIADB s'engage à traiter les données à caractère personnel exclusivement pour le compte du responsable de traitement et uniquement sur la base des instructions documentées qui lui sont communiquées.
ROCIADB ne détermine jamais les finalités des traitements réalisés pour le compte du responsable de traitement et n'utilise en aucun cas les données à caractère personnel à des fins propres, commerciales ou publicitaires.
Les traitements réalisés sont strictement limités à l'exécution des services prévus au contrat principal.

5.2 Respect des instructions documentées
ROCIADB traite les données personnelles uniquement sur instruction documentée du responsable de traitement.
Lorsque ROCIADB estime qu'une instruction est manifestement contraire au RGPD ou à toute autre disposition applicable en matière de protection des données personnelles, elle en informe sans délai le responsable de traitement et suspend, dans la mesure du possible, l'exécution de cette instruction jusqu'à réception de nouvelles directives.

5.3 Limitation des traitements
ROCIADB veille à ce que les traitements réalisés soient strictement limités à ce qui est nécessaire pour :
- Assurer le fonctionnement de la plateforme
- Assurer la maintenance corrective et évolutive
- Réaliser les sauvegardes
- Restaurer les données lorsque cela est nécessaire
- Garantir la sécurité des infrastructures

5.4 Personnel autorisé

ROCIADB veille à ce que les personnes autorisées à traiter des données personnelles :

- Soient spécifiquement habilitées
- Soient sensibilisées aux règles relatives à la protection des données
- Soient soumises à une obligation contractuelle ou légale de confidentialité
- N’accèdent aux données qu'en fonction de leurs missions

Les droits d'accès sont attribués selon le principe du moindre privilège et font l'objet de révisions périodiques.

5.5 Confidentialité

ROCIADB garantit la confidentialité des données à caractère personnel auxquelles elle peut avoir accès dans le cadre de l'exécution des services.

5.6 Accès exceptionnel aux données

Par principe, ROCIADB n'accède pas au contenu des données enregistrées par le responsable de traitement.

Toute consultation du contenu des données personnelles intervient uniquement lorsqu'elle est strictement nécessaire :

- À la résolution d'un incident technique
- À l'exécution d'une opération de maintenance
- À une demande d'assistance formulée par le responsable de traitement

Dans ce cas :

- L’accès est limité aux seules données nécessaires
- Seules les personnes habilitées peuvent intervenir
- La consultation est limitée à la durée strictement nécessaire

5.7 Documentation

ROCIADB tient à disposition du responsable de traitement les informations nécessaires permettant de démontrer le respect de ses obligations au titre du présent contrat.

Cette documentation peut notamment comprendre :

- Les politiques de sécurité applicables
- Les procédures internes
- La description des mesures techniques et organisationnelles

5.8 Évolution des mesures de sécurité

ROCIADB s'engage à maintenir un niveau de sécurité conforme.

Les mesures techniques et organisationnelles peuvent évoluer afin :

- D’améliorer la sécurité de la plateforme
- De tenir compte des évolutions technologiques
- De satisfaire aux exigences réglementaires

Toute évolution significative susceptible d'avoir un impact sur la sécurité des traitements est portée à la connaissance du responsable de traitement lorsqu'elle affecte les engagements contractuels.

5.9 Obligation générale de coopération
ROCIADB coopère de bonne foi avec le responsable de traitement afin de lui permettre de satisfaire à ses obligations issues du RGPD.

ARTICLE 6 – SÉCURITÉ DES TRAITEMENTS
6.1 Principe général
Conformément aux articles 28 et 32 du Règlement (UE) 2016/679, ROCIADB met en œuvre et maintient pendant toute la durée du contrat des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques présentés par les traitements réalisés pour le compte du responsable de traitement.
Ces mesures visent notamment à assurer :

- La confidentialité des données
- L'intégrité des données
- La disponibilité des traitements
- La résilience permanente des systèmes et services
- La capacité à rétablir rapidement la disponibilité des données en cas d'incident physique ou technique
- La protection contre tout accès, utilisation, modification, divulgation ou destruction non autorisés

6.2 Intégrité
ROCIADB met en œuvre les mesures nécessaires afin de prévenir toute altération non autorisée des données personnelles.
Les mécanismes de sécurité permettent notamment :

- D'assurer la traçabilité des opérations
- De limiter les risques d'altération accidentelle
- De détecter les anomalies de fonctionnement

6.3 Disponibilité
ROCIADB prend toutes mesures raisonnables afin d'assurer la disponibilité des services.
Ces mesures comprennent notamment :

- La supervision des infrastructures
- Les sauvegardes
- Les mécanismes de restauration
- La maintenance préventive
- La gestion des incidents

6.4 Amélioration continue
Les mesures techniques et organisationnelles sont régulièrement réévaluées afin de tenir compte :

- De l'évolution des risques
- Des évolutions technologiques
- Des recommandations de la CNIL
- Des retours d'expérience
- Des évolutions de la plateforme

Lorsque ces évolutions améliorent le niveau global de sécurité, elles peuvent être mises en œuvre sans qu'il soit nécessaire de modifier le présent contrat.

6.5 Documentation des mesures

Le détail des mesures techniques et organisationnelles mises en œuvre par ROCIADB figure en Annexe.

Cette annexe décrit notamment :

- La gouvernance de la sécurité
- La gestion des identités et des habilitations
- L'authentification
- Le contrôle des accès
- Le chiffrement
- La sécurité réseau
- L'hébergement
- Les sauvegardes
- La journalisation
- La gestion des incidents
- La télémaintenance
- Les procédures de développement sécurisé
- Les mesures de continuité d'activité

6.6 Limitation de l'obligation

Les parties reconnaissent que les mesures de sécurité mises en œuvre par ROCIADB ne dispensent pas le responsable de traitement de mettre en œuvre les mesures de sécurité relevant de sa propre responsabilité.

Le responsable de traitement demeure notamment responsable :

- De la gestion des comptes de ses utilisateurs
- De la confidentialité des identifiants communiqués à ses utilisateurs
- De la sécurité des postes de travail et terminaux utilisés pour accéder aux services
- De la sécurité de son propre réseau informatique

ARTICLE 7 – LOCALISATION DES DONNÉES ET TRANSFERTS INTERNATIONAUX

7.1 Hébergement des données

ROCIADB veille à ce que les données à caractère personnel confiées par le responsable de traitement soient hébergées au sein d'infrastructures offrant un niveau de sécurité adapté aux exigences du Règlement (UE) 2016/679.

Les données sont hébergées dans des centres de données situés au sein de l'Espace économique européen.

7.2 Absence de transfert international

ROCIADB s'engage à ne pas transférer les données personnelles vers un État situé en dehors de l'Espace économique européen sans avoir préalablement :

- Informé le responsable de traitement
- Mis en œuvre les garanties appropriées prévues par les articles 44 à 49 du RGPD

ARTICLE 8 – RECOURS À DES SOUS-TRAITANTS ULTÉRIEURS

8.1 Principe

Le responsable de traitement autorise ROCIADB à recourir à des sous-traitants ultérieurs lorsque leur intervention est nécessaire à l'exécution des services.

8.2 Garanties

ROCIADB sélectionne uniquement des prestataires présentant des garanties suffisantes en matière de sécurité, de confidentialité et de protection des données personnelles.
Avant toute collaboration, ROCIADB vérifie notamment :

- Les mesures techniques et organisationnelles mises en œuvre
- Les engagements contractuels du prestataire
- Les garanties offertes au regard du RGPD
- La localisation des traitements

ARTICLE 9 – ASSISTANCE AU RESPONSABLE DE TRAITEMENT

9.1 Principe général

Compte tenu de la nature des traitements réalisés et des informations dont il dispose, ROCIADB assiste le responsable de traitement afin de lui permettre de satisfaire aux obligations qui lui incombent en application du RGPD.
Cette assistance est fournie dans des conditions raisonnables et proportionnées, compatibles avec la nature des services souscrits.

9.2 Assistance relative aux droits des personnes concernées

ROCIADB met à disposition les fonctionnalités techniques permettant au responsable de traitement de répondre aux demandes d'exercice des droits des personnes concernées.
Lorsque ROCIADB reçoit directement une demande d'exercice des droits concernant des données traitées pour le compte du responsable de traitement, elle la transmet à celui-ci dans les meilleurs délais, sauf interdiction légale.
ROCIADB ne répond jamais directement aux personnes concernées, sauf instruction écrite du responsable de traitement.

ARTICLE 10 – EXERCICE DES DROITS DES PERSONNES CONCERNÉES

10.1 Principe

Le responsable de traitement demeure seul responsable du traitement des demandes relatives :

- Au droit d'accès
- Au droit de rectification
- Au droit à l'effacement
- Au droit à la limitation
- Au droit d'opposition
- Au droit à la portabilité
- Au droit de retirer son consentement

10.2 Assistance technique

ROCIADB met en œuvre les moyens techniques permettant, dans la mesure des fonctionnalités de la plateforme, de faciliter :

- La consultation des données
- Leur export
- Leur rectification
- Leur suppression
- Leur restitution

ARTICLE 11 – ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES (AIPD)

Le responsable de traitement demeure responsable de déterminer si les traitements qu'il met en œuvre nécessitent la réalisation d'une analyse d'impact relative à la protection des données.

Lorsque le responsable de traitement sollicite son assistance, ROCIADB met à disposition les informations nécessaires concernant :

- L'architecture de la plateforme
- Les mesures techniques et organisationnelles mises en œuvre
- Les mécanismes de sécurité
- Les modalités d'hébergement
- Les procédures de sauvegarde et de restauration

ROCIADB fournit les informations dont elle dispose, sans être tenue de réaliser elle-même l'analyse d'impact pour le compte du responsable de traitement.

ARTICLE 12 – VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

12.1 Détection des incidents

ROCIADB met en œuvre des procédures destinées à détecter, analyser et traiter tout incident de sécurité susceptible d'affecter les données personnelles traitées pour le compte du responsable de traitement.

12.2 Notification

Lorsqu'elle constate une violation de données personnelles concernant les traitements réalisés pour le compte du Responsable de traitement, ROCIADB en informe celui-ci dans les meilleurs délais et, dans toute la mesure du possible, dans un délai maximal de vingt-quatre (24) heures après en avoir eu connaissance.

12.3 Contenu de la notification

La notification comprend, lorsque ces informations sont disponibles :

- La nature de la violation
- Les catégories de données concernées
- Les catégories de personnes concernées
- Le nombre approximatif d'enregistrements concernés
- Les conséquences connues ou présumées de l'incident
- Les mesures déjà mises en œuvre
- Les mesures correctives envisagées

12.4 Coopération
ROCIADB coopère pleinement avec le responsable de traitement afin de lui permettre :
- D'évaluer les conséquences de la violation
- De prendre les mesures correctives nécessaires

ARTICLE 13 – AUDITS ET DÉMONSTRATION DE LA CONFORMITÉ
13.1 Obligation de coopération
ROCIADB met à la disposition du responsable de traitement toutes les informations raisonnablement nécessaires permettant de démontrer le respect des obligations qui lui incombent au titre du présent contrat et de l'article 28 du Règlement (UE) 2016/679.
Cette obligation peut être satisfaite notamment par la communication :
- Des politiques et procédures internes applicables
- De l'Annexe relative aux mesures techniques et organisationnelles
- De tout document permettant de démontrer la conformité des Services
-

13.2 Audits
Le responsable de traitement peut réaliser, ou faire réaliser par un auditeur indépendant soumis à une obligation de confidentialité, un audit portant sur les traitements réalisés pour son compte.
L'audit est limité aux traitements concernés par le présent contrat et réalisé une seule fois par an.

ARTICLE 14 – RESTITUTION, SUPPRESSION ET RÉVERSIBILITÉ DES DONNÉES
14.1 Fin des prestations
À l'expiration du contrat principal, quelle qu'en soit la cause, ROCIADB cesse tout traitement réalisé pour le compte du responsable de traitement, sous réserve des obligations légales de conservation qui lui sont applicables.

14.2 Restitution
Pendant la période contractuellement prévue, le responsable de traitement peut demander la restitution de ses données dans un format couramment exploitable, sous réserve des fonctionnalités disponibles au sein des services.

14.3 Suppression
À l'issue de la période de réversibilité prévue au contrat principal ou sur instruction du responsable de traitement, ROCIADB procède à la suppression des données personnelles, sauf lorsqu'une obligation légale impose leur conservation.

ARTICLE 15 – RESPONSABILITÉ
Chaque partie demeure responsable des obligations qui lui incombent en application du RGPD.
Le Responsable de traitement demeure seul responsable :
- De la licéité des traitements
- Des bases légales
- De l'information des personnes concernées
- Des données enregistrées dans la plateforme
- Des instructions adressées à ROCIADB

ROCIADB demeure responsable :

- Des traitements réalisés conformément aux instructions reçues
- De la sécurité des services
- Du respect des obligations qui lui incombent en qualité de sous-traitant.

ARTICLE 16 – DURÉE ET RÉSILIATION

Le présent contrat entre en vigueur à la date d'effet du contrat principal.
Il demeure applicable pendant toute la durée des traitements réalisés pour le compte du Responsable de traitement.
La cessation du contrat principal entraîne automatiquement la cessation du présent DPA, sous réserve des dispositions relatives :

- À la confidentialité
- À la responsabilité
- À la suppression ou à la restitution des données

Ces obligations demeurent applicables aussi longtemps que ROCIADB conserve des données pour le compte du responsable de traitement.

ARTICLE – 17 DROIT APPLICABLE ET JURIDICTION COMPÉTENTE

Le présent contrat est régi par le droit français.
Les parties s'engagent à rechercher une solution amiable à tout différend relatif à son interprétation ou à son exécution.
À défaut d'accord amiable dans un délai raisonnable, tout litige sera porté devant les juridictions matériellement compétentes du ressort de la Cour d'appel dont dépend le siège social de ROCIADB.

ARTICLE 18 – MODIFICATION DU PRÉSENT CONTRAT

ROCIADB peut modifier le présent contrat lorsque cette modification est rendue nécessaire par :

- Une évolution de la réglementation applicable
- Une décision d'une autorité de contrôle
- Une évolution des services
- Une amélioration des mesures techniques et organisationnelles

Toute modification ayant un impact substantiel sur les droits ou obligations des parties est portée à la connaissance du responsable de traitement avant son entrée en vigueur
Lorsque la modification résulte d'une obligation légale ou réglementaire, elle s'applique à compter de sa date d'entrée en vigueur.

ARTICLE 19– DISPOSITIONS FINALES

Le présent contrat constitue l'intégralité de l'accord des parties concernant le traitement des données à caractère personnel réalisé dans le cadre des services.
Si une stipulation du présent contrat est déclarée nulle ou inapplicable, les autres stipulations demeurent pleinement en vigueur.

ANNEXE
Mesures Techniques et Organisationnelles de Sécurité

1. Gestion des identités et authentification

ROCIADB met en œuvre une politique d'authentification destinée à garantir que seuls les utilisateurs autorisés puissent accéder aux services.
Les mesures comprennent notamment :

- Création automatisée des comptes utilisateurs via un formulaire d'inscription sécurisé
- Comptes utilisateurs nominatifs
- Stockage des mots de passe exclusivement sous forme hachée et salée
- Impossibilité pour les administrateurs ou les équipes techniques de consulter les mots de passe des utilisateurs
- Politique de complexité imposant un minimum de huit caractères comprenant des lettres majuscules, des lettres minuscules, des chiffres et des caractères spéciaux
- Authentification multifacteur disponible pour les utilisateurs et obligatoire pour les comptes administrateurs
- Archivage des comptes inactifs selon la politique de gestion du cycle de vie des comptes

2. Gestion des habilitations

Les accès aux traitements sont limités aux seules personnes habilitées.
Les habilitations sont attribuées selon les missions confiées et le principe du moindre privilège.
Les comptes disposant de droits d'administration font l'objet d'un contrôle particulier.
Les habilitations sont revues périodiquement et supprimées lorsqu'elles ne sont plus nécessaires.

3. Protection des données hébergées

La plateforme permet aux clients d'enregistrer les données nécessaires à leurs activités.
ROCIADB n'effectue aucun contrôle préalable du contenu des données déposées par ses clients.
Les clients demeurent seuls responsables de la nature des données enregistrées.
Lorsque des catégories particulières de données sont hébergées, celles-ci sont traitées exclusivement dans le cadre des prestations confiées par le Responsable de traitement.

4. Télémaintenance et support

Les opérations de support sont réalisées exclusivement dans le cadre des prestations contractuelles.
Les interventions sont limitées :

- Aux données nécessaires
- Aux personnes habilitées
- À la durée de l'intervention

Aucune copie durable des données n'est réalisée dans le cadre des opérations de support.

5. Hébergement

Les infrastructures de production sont hébergées par OVHcloud.
Les données sont hébergées au sein de l'Union européenne, sauf demande expresse du Responsable de traitement.
L'hébergement repose sur une infrastructure cloud sécurisée.

6. Sécurité des communications

Les échanges entre les utilisateurs, les API et les infrastructures sont protégés au moyen de protocoles de chiffrement conformes à l'état de l'art.
Les communications utilisent le protocole TLS version 1.2 minimum.

7. Cloisonnement des données

Les environnements des différents clients sont logiquement isolés.
Chaque client dispose de son propre espace de traitement (tenant).
Les mécanismes de cloisonnement empêchent tout accès non autorisé entre plusieurs environnements clients.

8. Journalisation

Les opérations techniques font l'objet d'une journalisation destinée à assurer la traçabilité des interventions et la détection des incidents.
Les journaux sont accessibles uniquement aux développeurs habilités.
Les logs techniques sont stockés sur un espace S3 hébergé par OVHcloud.
Les journaux ne contiennent pas de données personnelles directement identifiantes.

9. Sauvegardes

Des mécanismes de sauvegarde sont mis en œuvre afin d'assurer la disponibilité des données et la continuité des services.
Les sauvegardes sont protégées contre tout accès non autorisé.

10. Développement sécurisé

Le développement de la plateforme repose sur des pratiques destinées à garantir la sécurité des applications.
Les mises à jour correctives et évolutives sont déployées selon une procédure maîtrisée.
Les composants logiciels sont maintenus à jour afin de limiter les risques liés aux vulnérabilités connues.