

Pacte de sécurité

Nos engagements de confidentialité et de sécurité

Ce document présente les engagements que Dotris prend envers ses clients concernant la confidentialité, la protection et la sécurité des informations qui lui sont confiées. Il s'applique dès le premier échange, avant même la signature de tout contrat.

1. Confidentialité dès le premier échange

Toute information que vous nous communiquez, à l'oral comme à l'écrit, est traitée comme confidentielle à compter du premier contact. Cela couvre vos processus métier, vos données commerciales et financières, vos difficultés opérationnelles, l'architecture de vos systèmes et tout élément que vous nous exposez pour évaluer votre besoin.

Concrètement, nous nous engageons à :

- Ne divulguer aucune information vous concernant à un tiers sans votre accord écrit préalable.
- Ne pas utiliser vos informations à d'autres fins que l'étude et la réalisation de votre projet.
- Ne citer ni votre nom, ni votre marque, ni votre projet en référence commerciale sans votre autorisation expresse.
- Maintenir cette confidentialité même si le projet ne se concrétise pas.

2. Accès à vos données

Nous appliquons le principe du moindre privilège : nous accédons uniquement aux données nécessaires à la mission, pour la durée nécessaire, et uniquement par les personnes qui y travaillent.

- Les accès à vos systèmes sont nominatifs et tracés.
- Nous privilégions systématiquement les environnements de test et les jeux de données anonymisés lorsque la mission le permet.
- Nous vous demandons les accès de production uniquement lorsqu'ils sont indispensables, et nous vous en expliquons la raison.
- Chaque accès qui n'est plus nécessaire est révoqué, et l'ensemble des accès est révoqué en fin de mission.

3. Sécurité technique

La sécurité est intégrée dès la conception des solutions que nous construisons, et non ajoutée après coup.

Protection des échanges et des données

- Chiffrement systématique des flux en transit (HTTPS/TLS).
- Chiffrement des données sensibles au repos.
- Bases de données isolées du réseau public.
- Cloisonnement strict entre les environnements de développement, de recette et de production.

Gestion des secrets et des accès

- Les clés d'API, mots de passe et certificats sont stockés dans un coffre-fort dédié et ne sont jamais inscrits dans le code source.
- Authentification par jetons avec gestion fine des droits, afin que chaque utilisateur n'accède qu'aux informations qui le concernent.
- Authentification à double facteur activée sur nos propres outils et sur les accès que nous détenons chez vous.

Développement et maintenance

- Chaque modification de code passe par une pipeline d'intégration continue : tests automatisés, analyse statique et revue de code.
- Les déploiements sont automatisés, tracés et réversibles.
- Les dépendances logicielles sont surveillées en continu afin de détecter les vulnérabilités connues.

4. Hébergement et localisation

Nous hébergeons les applications que nous développons sur des infrastructures cloud professionnelles, avec des données localisées dans l'Union européenne, sauf demande contraire de votre part.

5. Recours à des services tiers

Certaines solutions font appel à des services externes, notamment pour les fonctionnalités d'intelligence artificielle. Dans ce cas :

- Nous vous informons en amont des services concernés et de la nature des données qui y transitent.
- Nous retenons des offres professionnelles assorties d'un engagement contractuel de non-rétention et de non-utilisation de vos données pour l'entraînement des modèles.
- Lorsque votre niveau d'exigence le requiert, nous déployons des modèles auto-hébergés sur votre propre infrastructure, afin qu'aucune donnée ne quitte votre périmètre.
- Aucun service tiers n'est introduit dans votre solution sans votre validation.

6. Propriété et réversibilité

- **Confidentialité et propriété des données** : Vos informations, données et contenus restent votre propriété entière. Ils sont strictement confidentiels, utilisés uniquement dans le cadre de la mission et ne sont jamais réutilisés, revendus ou intégrés dans d'autres modèles ou projets.
- **Réversibilité et transparence** : La solution est développée sur des technologies standards du marché et documentée, afin de garantir sa maintenabilité et sa reprise par d'autres équipes. Vous conservez la pleine maîtrise de vos clés, de vos accès et de vos documentations techniques.
- **Restitution et suppression** : À la fin de la mission, nous vous remettons l'ensemble des livrables et procédons à la suppression de vos données de nos environnements de travail, sur votre demande ou dans un délai convenu ensemble.

7. Conformité au RGPD

Lorsque nous traitons des données à caractère personnel pour votre compte, nous intervenons en qualité de sous-traitant au sens du Règlement général sur la protection des données.

- Nous traitons ces données uniquement sur votre instruction documentée.
- Nous mettons en œuvre les mesures techniques et organisationnelles décrites dans ce document.
- Nous vous assistons dans l'exercice des droits des personnes concernées et dans vos obligations de sécurité.
- Un accord de sous-traitance dédié est signé lorsque la mission implique le traitement de données personnelles.

8. Gestion des incidents

En cas d'incident de sécurité affectant vos données ou vos systèmes, nous nous engageons à vous en informer sans délai injustifié, à vous communiquer les éléments dont nous disposons sur la nature et l'étendue de l'incident, et à coopérer pleinement aux mesures de remédiation.

9. Personnes engagées

Les engagements du présent document lient l'ensemble des personnes intervenant pour Dotris sur votre projet, y compris les collaborateurs, stagiaires et prestataires indépendants, qui sont tenus aux mêmes obligations de confidentialité.

10. Durée

Les engagements de confidentialité prennent effet dès le premier échange et se poursuivent pendant toute la durée de la mission ainsi qu'après son terme.

Contact

Pour toute question relative à ce document ou à la sécurité de vos données :

contact@dotris.fr

Engagement des parties

Le présent pacte de sécurité est remis au client préalablement à tout échange d'informations confidentielles. Il peut être contresigné par les deux parties.

Pour Dotris Nom et fonction : Date : Signature :	Pour le client Nom et fonction : Date : Signature :
--	---