

SÉCURITÉ & CONFORMITÉ

Nous travaillons pour des banques, un acteur de la santé et un éco-organisme. Dans ces secteurs, l'homologation d'un prestataire précède le contrat, et elle porte sur des points précis. Ce document y répond avant que la question soit posée.

FORMALISÉE, SIGNÉE PAR LA DIRECTION

Notre politique de sécurité de l'information, en cinq axes

- 1** **Sécurisation du patrimoine numérique.** Confidentialité, intégrité, disponibilité, authenticité, traçabilité et non-répudiation. Ces propriétés encadrent aussi bien les données que nos clients nous confient que les travaux de notre pôle recherche et développement.
- 2** **Gouvernance et conformité.** Protection des données personnelles, classification de l'information selon quatre niveaux de sensibilité – publique, interne, confidentielle, secrète – avec les mesures correspondantes, et conformité réglementaire.
- 3** **Maîtrise des accès.** Principe du moindre privilège, authentification forte, sécurisation des accès nomades. Avec des équipes réparties sur plusieurs sites et une part de télétravail assumée, c'est un point que nous traitons sérieusement plutôt que de le contourner.
- 4** **Sécurité de l'écosystème et résilience.** Clauses de sécurité, engagements de service, obligations de confidentialité et droit d'audit dans les contrats de nos sous-traitants. Un processus formel de détection, signalement, analyse et correction des incidents, avec communication transparente en cas d'impact.
- 5** **Culture de sécurité.** Tous nos collaborateurs sont formés aux bonnes pratiques, aux risques d'hameçonnage et d'ingénierie sociale. Une politique que personne n'applique ne protège rien.

14.05.26

DPO déclaré à la CNIL. Prise d'effet de la désignation. Coordonnées publiques tenues à disposition par la CNIL.

5 AXES

Politique de sécurité formalisée et signée par la direction. RSSI nommé.

72 H

Délai de réponse aux questionnaires d'homologation, en heures ouvrées.

Trois rôles nommés

Un responsable de la sécurité des systèmes d'information, un délégué à la protection des données déclaré à la CNIL, et un référent anti-corruption. Dans une entreprise de vingt-cinq personnes, la question n'est pas de savoir si ces rôles existent sur un organigramme, mais qui les porte – et ils sont nommés.

Protection des données personnelles

Un DPO déclaré à la CNIL

Mindcross a désigné son délégué à la protection des données auprès de la CNIL, avec prise d'effet au **14 mai 2026**. Ses coordonnées publiques sont tenues à disposition par la CNIL ; il est joignable directement à dpo@mindcross.fr.

Une indépendance formalisée

Sa lettre de mission prévoit un rattachement direct au dirigeant, l'absence de toute instruction dans l'exercice de ses missions, et l'impossibilité d'être pénalisé dans sa carrière à raison de celles-ci. Ce sont les exigences des articles 37 à 39 du RGPD, et elles sont écrites.

Un dispositif en fonctionnement

- Registre des traitements tenu à jour
- Analyses d'impact conduites lorsqu'elles sont nécessaires
- Procédure formelle de notification des violations de données
- Toute demande d'exercice de droits transférée au DPO **sous vingt-quatre heures**, quel que soit le canal, puis traitée dans les délais légaux
- Vérification d'identité limitée au doute raisonnable, avec suppression immédiate du justificatif

AU-DELÀ DE LA SÉCURITÉ TECHNIQUE

Conformité financière et éthique

- **Lutte contre le blanchiment et le financement du terrorisme.** Procédure interne comportant une classification des risques, la vérification des bénéficiaires effectifs, la détection des situations financières atypiques et des contrôles internes.
- **Anti-corruption.** Tolérance zéro sur la corruption et les conflits d'intérêts, conformément au dixième principe du Pacte mondial des Nations Unies. Un référent est nommé.
- **Vigilance sur la chaîne de sous-traitance.** Pré-qualification documentée, classification par niveau de risque, clauses contractuelles de vigilance et droit d'audit.

NOTRE DOSSIER FOURNISSEUR

Les documents qui répondent à l'essentiel des grilles

[Politique de sécurité de l'information](#)[Charte informatique](#)[Lettre d'engagement cyber](#)[Support de sensibilisation cybersécurité](#)[Procédure LCB-FT](#)[Politique de gestion des risques fournisseurs](#)

Ils sont présentés dans le cadre d'une homologation fournisseur.

Notre engagement de réponse

Si une question ne trouve pas sa réponse dans ces documents, écrivez-nous : **soixante-douze heures ouvrées**. C'est un engagement calibré pour être tenu un vendredi soir comme pendant des congés – dans un cycle d'homologation où les prestataires répondent en semaines.