Checklist Sécurité Dataroom IA

Alignée RGPD & ISO 27001

- ☐ Cartographie des données et classification.
- ☐ Chiffrement AES-256 au repos et TLS 1.3 en transit.
- ☐ Stockage et traitement de la donnée exclusivement dans l'UE (Art. 44 RGPD).
- ☐ Contrôles d'accès RBAC et authentification multifacteur (MFA).
- ☐ Journalisation immuable et conservation 12 mois minimum.
- ☐ Audit annuel ISO 27001 & rapport SOC 2 Type II.
- ☐ Analyse d'impact sur la protection des données (DPIA) préalable.
- ☐ Plan de réponse aux incidents < 24 h & tests semestriels.
- ☐ Durcissement et supervision continue du pipeline IA (poisoning, model theft).
- ☐ Revue humaine des décisions automatisées (Art. 22 RGPD).
- ☐ Segregation logique entre tenants & clés uniques par client.
- ☐ Sauvegardes chiffrées, tests de restauration trimestriels.
- ☐ Rotation trimestrielle des clés KMS et gestion de secrets.
- ☐ Conformité aux guides CNIL IA & Cloud.
- ☐ Due diligence fournisseurs & accord DPA signé