

Checklist RGPD pour SaaS

Produit, contrats, fournisseurs et preuves clients

Cette checklist aide les équipes produit, sécurité et ventes à préparer les éléments demandés par des clients européens.

1. Produit et données

Flux de collecte, import, support, logs, sauvegarde et suppression cartographiés

Preuve / note :

Rôles responsable/sous-traitant qualifiés par finalité

Preuve / note :

Données de test minimisées ou synthétiques

Preuve / note :

Fonctionnalités IA et analytics inventoriées

Preuve / note :

2. Contrats

DPA conforme à l'article 28

Preuve / note :

Instructions et finalités définies

Preuve / note :

Assistance droits, incidents et AIPD décrite

Preuve / note :

Audit et fin de contrat encadrés

Preuve / note :

Liste des sous-traitants ultérieurs publiée ou disponible

Preuve / note :

3. Hébergement et transferts

Pays d'hébergement, sauvegarde, support et administration connus

Preuve / note :

Mécanisme de transfert documenté

Preuve / note :

TIA et mesures supplémentaires préparées si nécessaires

Preuve / note :

Changements de localisation soumis à une revue

Preuve / note :

4. Sécurité et exploitation

MFA et gestion des accès privilégiés

Preuve / note :

Chiffrement et gestion des clés documentés

Preuve / note :

Journalisation, sauvegardes et continuité testées

Preuve / note :

Procédure d'incident et canal client définis

Preuve / note :

Conservation et suppression automatisables

Preuve / note :

5. Preuves de vente

Questionnaire sécurité/RGPD validé

Preuve / note :

Schéma de flux compréhensible

Preuve / note :

Résumé des mesures disponible

Preuve / note :

Contacts DPO/sécurité identifiés

Preuve / note :

Réponses cohérentes avec les contrats et le produit

Preuve / note :

Cette checklist ne constitue pas une certification ni une garantie de conformité. Faites valider les conclusions par les personnes compétentes.