# Compte rendu RGPD

## 1. Désigner un pilote (DPO – Délégué à la protection des données)

- Désignation : M. Auguste Klin ou une personne compétente désignée en interne/externe.

- Rôle : Accompagner la mise en conformité, contrôler, conseiller, être point de contact avec la CNIL et les usagers.

- Documentation : Fiche de désignation conservée en interne.

## 2. Cartographier les traitements de données

Données collectées via l'application web :

- Données d'identité : nom, prénom, adresse e-mail, téléphone.

- Données de connexion : identifiants de compte.

- Données liées aux formations : historique d’inscriptions, pré requis remplis, factures, équipements déclarés.

- Données de paiement : état du paiement (confirmation ou non).

Finalités :

- Création de comptes et gestion des inscriptions.

- Paiement, facturation, suivi des formations.

- Communication avec les stagiaires.

- Mise en liste d’attente et relance en cas d’annulation.

## 3. Prioriser les actions à mener

Risques principaux :

- Perte ou fuite de données personnelles.
- Accès non autorisé aux comptes ou données de paiement.
- Non-respect des droits des personnes.

Actions prioritaires :

- Mise en place d’une politique de mots de passe robustes.
- Stockage sécurisé (chiffrement des mots de passe).
- Accès restreint aux données selon les rôles (formateur/admin).
- Détection d’intrusions et tests de sécurité.

## 4. Gérer les risques

Scénarios de risques :

- Intrusion via internet (DMZ ouverte).
- Suppression accidentelle des données de formation.
- Interception des paiements ou usurpation d’identité.

Mesures proposées :

- Connexion en HTTPS (chiffrement SSL/TLS).
- Sauvegarde hebdomadaire automatique de la base.
- VPN pour accès distant sécurisé.
- Liste blanche d’IP pour accès FTP/SSH.
- Installation d’un IDS (système de détection d’intrusion).

- Mise en place d’un système de basculement sur un 2e serveur web.

## 5. Encadrer les traitements de données

- Clauses de confidentialité dans les contrats de développement.
- Contrat avec hébergeur (si hébergement externe) conforme RGPD.
- Données personnelles non transférées hors UE.
- Limitation de conservation : 3 ans après la dernière activité de l'utilisateur.

## 6. Informer les personnes et recueillir leur consentement

- Politique de confidentialité affichée sur le site.
- Consentement explicite pour la création de compte.
- Informations sur les droits RGPD dans les e-mails de confirmation.

Droits rappelés :

- Droit d’accès, de rectification, de suppression.
- Droit à la portabilité et à l’opposition.
- Droit de réclamation auprès de la CNIL.

## 7. Organiser les procédures internes

- Procédure de gestion des violations de données (notification à la CNIL <72h).
- Registre des traitements mis à jour.
- Formation des membres de l’équipe Easy Bee sur la protection des données.