**QUESTIONNAIRE A L’ATTENTION DES PRESTATAIRES**

**Protection des Données Personnelles et sécurité informatique**

1. **Identification de la Société :**

Adresse :

Code postal

Ville :

Téléphone :

Nom du responsable de traitement :

Responsable informatique / RSSI :

Nom, prénom

Contact /DPO :

Contact juridique :

1. **Politique de protection des données**

Avez-vous mis en place une gouvernance en matière de protection des données au sein de votre entreprise ?

Avez-vous mis en place une politique interne formalisée de protection des données ?

Avez-vous mis en place une politique externe formalisée de protection des données ?

Tenez-vous un registre des traitements mis en œuvre ?

Avez-vous intégré le principe du Privacy by design dans le cadre de vos activités ?

Avez-vous désigné un data protection officer au sein de votre entreprise ou de votre groupe ?

Avez-vous sensibilisé vos salariés sur la protection des données ?

Avez-vous mis en place une procédure de gestion des droits des personnes ?

Avez-vous adopté une procédure de gestion en cas d’incident de sécurité, en cas d violations de données à caractère personnel ?

Avez-vous obtenu un Label délivré par une autorité de contrôle (telle que la Cnil) ?

**3. Sécurité Informatique**

**A) Politique**

Avez-vous une politique de sécurité ?

Disposez-vous d’une politique de mot de passe ?

Etes-vous certifié ou labellisé en matière de sécurité ?

Avez-vous un RSSI au sein de votre entreprise ?

Existe-il un encadrement contractuel opposable aux salariés et tiers intervenant dans le cadre des prestations ? (Clause de confidentialité, charte informatique etc…)

Réalisez-vous des audits de sécurité interne et/ou externe ? Si oui, à quelle périodicité ?

Si vous avez contracté une assurance contre risques de cyber-attaque, pouvez-vous préciser le type de risques couverts ?

**B) Pratique**

Les serveurs utilisés pour le traitement des données sont-ils accessibles depuis internet (pas de firewall, pas de DMZ) ? sont-ils connectés sur des systèmes d’information externes ?

Etes-vous en mesure de faire une analyse de sécurité à notre demande ?

Utilisez-vous des comptes génériques pour l’accès aux serveurs ou applications gérant le traitement des données ?

Avez-vous une stratégie de mise à jour de votre infrastructure (OS, patchs, antivirus). Si oui, laquelle ?

Avez-vous un anti-virus sur chaque serveur ?

Quelle est la fréquence de mise à jour ? Avez-vous un anti-virus sur chaque poste de travail ?

Quelle est la fréquence de mise à jour ?

Si ce n’est pas déjà fait, accepteriez-vous de mettre en place un test d’intrusion annuel avec un partenaire externe ?

**C) Stockage du fichier et des données**

Cette série de questions vise à estimer la vulnérabilité des données qui vous sont confiées, lorsqu'elles figurent sur votre réseau pour les nécessités du traitement

Lors du traitement, les données sont-elles stockées, même temporairement hors de l’union européenne ?

Si oui, dans quels pays seront stockées les informations ?

Veuillez préciser la liste des sites où sont stockées les données ? (Site primaire, backup, etc…)

Nom et adresse de la société hébergeant les données ?

Cette société d’hébergement dispose-t-elle d’une certification ? si oui, laquelle ?

Assurez-vous la gestion des infrastructures et des systèmes hébergeant les données ?

Assurez-vous la gestion des applications manipulant les données ?

Les données sont-elles stockées sur des équipements qui vous sont dédiés ?

Les données sont-elles stockées sur des équipements qui nous sont dédiés ?

Les machines du traitement sont-elles dédiées au traitement des fichiers sensibles ?

Quelles mesures de sécurité sont mises en œuvre s’agissant du stockage des données ?

En cas de problème, pourriez-vous récupérer les données ? Si oui, quelle est la méthode de récupération des données ?

Date

Signature