**Annexe 2 à l’acte d’engagement – Marché n° MA 25 SI 0006**

**QUESTIONNAIRE RGPD**

**Realisation de prestations de maintenance du site intranet des salaries de filieris**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Objet | **Question** | **Oui** | **Non** | **Commentaires** |
| ***1. Politique de Sécurité*** | 1.1 Avez-vous désigné un responsable de la sécurité de votre système d'information (RSSI) ? |  |  |  |
| 1.2 Procédez-vous périodiquement à une analyse des risques liés à vos Systèmes d'Information? |  |  |  |
| 1.3 Disposez-vous d'une politique de sécurité des Systèmes d'Information (PSSI) actualisée, associée à un plan d’actions mis à jour régulièrement ? |  |  |  |
| 1.4 Avez-vous mis en œuvre un Système de Management de la Sécurité de l'Information (de type ISO 27001) ? |  |  |  |
| 1.5 Avez-vous formalisé un Plan d’Assurance Sécurité conforme aux recommandations de l’ANSSI ? |  |  |  |
| ***2. Inventaire des actifs*** | 2.1 Disposez-vous d'une documentation concernant l'inventaire des actifs contenant les données personnelles de vos Clients par système ? |  |  |  |
| 2.2 Cette documentation permet-elle de les identifier et de les localiser ? |  |  |  |
| ***3. Maîtrise des accès*** | 3.1 Avez-vous formalisé une politique de contrôle d’accès (gestion des identités, robustesse des mots de passe, procédure d’habilitations, revue des comptes…) |  |  |  |
| 3.2 Votre charte informatique contient-elle des clauses liées au secret professionnel et à la confidentialité des données à caractère personnel ? |  |  |  |
| 3.2 Avez-vous mis en œuvre un programme régulier de formation et sensibilisation de vos collaborateurs concernant la protection des données de vos Clients ? |  |  |  |
| 3.4 Les contrats avec d'autres Tiers qui peuvent potentiellement avoir accès à nos données intègrent-ils des obligations de protection des données à caractère personnel? |  |  |  |
| 3.5 Avez-vous mis en œuvre un contrôle de ces obligations de protection ? |  |  |  |
| ***4. Sécurité physique*** | * 4.1 Existe-t-il une politique de sécurité physique mise en place par votre société avec des règles différenciées suivant la criticité des locaux ? |  |  |  |
| * 4.2 Procédez-vous à des vérifications sur les droits d'accès physiques à vos locaux ? |  |  |  |
| ***5. Incident*** | 5.1 Existe-t-il une procédure formalisée sur la gestion des incidents (détection, analyse, plan d'action, recensement dans une base...)? |  |  |  |
| 5.2 Procédez-vous à l'enregistrement et à l'analyse des incidents informatiques, notamment sur les données à caractère personnel ? |  |  |  |
| 5.3 Existe-t-il une procédure de remontée d'alerte formalisée vers vos Clients en cas d'incident informatique ? |  |  |  |
| 5.4 Existe-t-il une procédure de remontée formalisée vers vos Clients en cas de violation de données à caractère personnel ? |  |  |  |
| ***6. Continuité d’activité*** | 6.1 Avez-vous défini un plan de continuité d'activité (PCA) ? |  |  |  |
| 6.2 Les sauvegardes des données à caractère personnel sont-elles garanties selon une procédure de tests de restauration ? |  |  |  |
| 6.3 Votre Plan de reprise d’activité (PRA) fait-il l’objet de tests annuels ? |  |  |  |
| ***7. Protection des données à caractère personnel*** | 7.1 Avez-vous désigné un délégué à la protection des données (DPD/DPO) ? |  |  |  |
| * 7.2 Procédez-vous à une analyse des risques concernant les données à caractère personnel de vos clients ? |  |  |  |
| * 7.3 Disposez-vous une Politique de protection des données à caractère personnel ? |  |  |  |
| * 7.4 Avez-vous formalisé une procédure permettant de garantir l’information des personnes concernées et de donner suite à leurs demandes d’exercice des droits ? |  |  |  |
| * 7.5 Avez-vous mis en œuvre une approche de protection des données personnelles de vos Clients dans les projets (notions de « privacy by design » et « privacy by default ) ? |  |  |  |
| * 7.6 Tenez-vous à jour un registre des traitements de données à caractère personnel |  |  |  |
| ***8. Contrôle interne et Audits*** | 1. 8.1 Votre société dispose-t-elle d'un contrôle interne de bonne application des politiques de sécurité et de conformité ? |  |  |  |
| * 8.2 Réalisez-vous périodiquement des audits techniques d’intrusions sur votre réseau et dans vos systèmes ? |  |  |  |
| 8.3 Votre société fait-elle l'objet d'audits périodiques sur les problématiques de sécurité de l'information et de protection des données à caractère personnel ? |  |  |  |
| ***9. Traitement ou échange de données à caractère personnel sensibles*** | 9.1 Avez-vous un agrément Hébergeur de données de Santé |  |  |  |
| 9.2 Etes-vous certifié Hébergeur de données de Santé ? |  |  |  |
| 9.3 Etes-vous certifié Hébergeur de données de Santé ? |  |  |  |
| 9.4 Avez-vous formalisé une politique de chiffrement des données de vos Clients ? |  |  |  |
| 9.5 Disposez-vous de solutions pour échanger de façon sécurisée des données sensibles avec des tiers ? |  |  |  |
| ***10. Autre élément relatif à la sécurité ou protection des données à caractère personnel pouvant nous intéresser*** |  | | | |