**Annexe n° 5 à l’acte d’engagement – Marché n° AO 25 SI 0007**

**QUESTIONNAIRE RGPD**

**Mise à disposition d’un service de réseau de données et de téléphonie et prestations associées pour les besoins de Filieris**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Objet | **Question** | **Oui** | **En cours** | **A planifier** | **Non** | **Commentaires** |
| ***1. Politique de Sécurité*** | 1.1 Disposez-vous d'une politique de sécurité ? (Politique de sécurité des Systèmes d'Information ou Politique de sécurité de 'information) ? |  |  |  |  |  |
| * 1.2 En avez-vous déduit des règles de sécurité (politiques par thème sécurité, procédures techniques,..) ? |  |  |  |  |  |
| * 1.3 Avez-vous désigné un responsable de la sécurité de votre système d'information (RSSI) ? |  |  |  |  |  |
| * 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 défini un plan de continuité d'activité (PCA) ? |  |  |  |  |  |
| * 1.6 Votre PRA fait-il l’objet de tests périodiques ? |  |  |  |  |  |
| ***2. Données personnelles*** | 2.1 Avez-vous procéder à une analyse des risques concernant les données personnelles de vos clients ? |  |  |  |  |  |
| * 2.2 Avez-vous désigné un CIL ou un DPD/DPO? |  |  |  |  |  |
| * 2.3 Avez-vous mis en œuvre un programme de formation et sensibilisation de vos collaborateurs concernant la protection des données personnelles de vos Clients ? |  |  |  |  |  |
| * 2.4 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 ) ? |  |  |  |  |  |
| **Objet** | **Question** | **Oui** | **En cours** | **A planifier** | **Non** | **Commentaires** |
| ***3. Chiffrement*** | * 3.1 Avez-vous formalisé une politique de chiffrement des données de vos Clients ? |  |  |  |  |  |
| * 3.2 Disposez-vous de solutions pour échanger de façon sécurisée des données personnelles ou sensibles avec des tiers ? |  |  |  |  |  |
| ***4. Incident*** | * 4.1 Existe-t-il une procédure formalisée sur la gestion des incidents (détection, analyse, plan d'action, recensement dans une base...)? |  |  |  |  |  |
| * 4.2 Procédez-vous à l'enregistrement et à l'analyse des incidents informatiques, notamment sur les données personnelles ? |  |  |  |  |  |
| * 4.3 Existe-t-il une procédure de remontée d'alerte formalisée vers vos Clients en cas d'incident sur leurs données personnelles? |  |  |  |  |  |
| ***5. Contrôle*** | 1. 5.4 Votre société dispose-t-elle d'un contrôle interne qui adresse les problématiques de sécurité de l'information et de protection des données personnelles? |  |  |  |  |  |
| ***6. Audit*** | * 6.1 Votre société fait-elle l'objet d'audits périodiques sur les problématiques de sécurité de l'information et de protection des données personnelles? |  |  |  |  |  |
| ***7. Audits techniques*** | 7.1 Réalisez-vous périodiquement des tests de détection des intrusions dans vos systèmes ? |  |  |  |  |  |
| ***8. Inventaire des actifs*** | * 8.1 Disposez-vous d'une documentation concernant l'inventaire des actifs contenant les données personnelles de vos Clients par système ? |  |  |  |  |  |
| 8.2 Cette documentation permet-elle de les identifier et de les localiser ? |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Objet** | **Question** | **Oui** | **En cours** | **A planifier** | **Non** | **Commentaires** |
| ***9. Gestion de vos prestataires*** | * 9.1 Les contrats avec d'autres Tiers qui peuvent potentiellement avoir accès à nos données intègrent-ils des obligations de protection des données personnelles ? |  |  |  |  |  |
| * 9.2 Avez-vous mis en œuvre un contrôle de ces obligations de protection ? |  |  |  |  |  |
| ***10. Sécurité physique*** | * 10.1 Existe-t-il une politique de sécurité physique mise en place par votre société avec des règles différenciées suivant la criticité des locaux ? |  |  |  |  |  |
| * 10.2 Procédez-vous à des vérifications sur les droits d'accès physiques à vos locaux ? |  |  |  |  |  |
| ***11. Autre élément relatif à la sécurité ou protection des données personnelles pouvant nous intéresser*** |  |  |  |  |  |  |