**ANNEXE 2 À L’ATTRI1 (ACTE D’ENGAGEMENT)**

**N°25 AC 07**

**PRESTATIONS DE SERVICES D’ACHEMINEMENT ET DE DISTRIBUTION DE COURRIERS POUR LE COMPTE DES CENTRES ÉDITIQUES DE LA SÉCURITÉ SOCIALE**

**Nom et adresse du prestataire :**

**Cachet de l’entreprise et signature du responsable :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Objet*** | Question | Oui | Non | Commentaires |
| ***Données personnelles*** | Avez-vous un registre des traitements des données personnelles effectués pour le compte de vos clients ? |  |  |  |
|  | Avez-vous désigné un DPO (délégué à la protection des données) ? |  |  |  |
|  | * Avez-vous un RSSI désigné ou une personne responsable de la sécurité de votre SI ? |  |  |  |
|  | * Avez-vous mis en œuvre un programme de formation et sensibilisation de vos collaborateurs concernant la protection des données personnelles de vos Clients au cours des 12 derniers mois ? |  |  |  |
|  | * Avez-vous mis en place des formations/sensibilisation à la sécurité des SI auprès de vos collaborateurs au cours des 12 derniers mois |  |  |  |
|  | * Disposez-vous d’une politique de confidentialité et de protection des données personnelles ? |  |  |  |
|  | Avez-vous mis en place des actions pour répondre aux droits des personnes, aux demandes de consultation, de rectification, ou de suppression de leurs données ? |  |  |  |
| ***Localisation des données*** | Les données personnelles sont hébergées dans la communauté européenne ? Préciser le pays |  |  |  |
| ***Politique de Sécurité*** | Disposez-vous d'une politique de sécurité ? (Politique de sécurité des Systèmes d'Information ou Politique de sécurité de l'information) ? |  |  |  |
|  | * Avez-vous défini un plan de continuité d'activité (PCA) ? |  |  |  |
| ***Chiffrement*** | * Avez-vous formalisé une politique de chiffrement des données de vos Clients ? |  |  |  |
|  | * Disposez-vous de solutions pour échanger de façon sécurisée des données personnelles ou sensibles avec des tiers ? |  |  |  |
| ***Incident*** | * Existe-t-il une procédure formalisée sur la gestion des incidents (détection, analyse, plan d'action, recensement dans une base...)? |  |  |  |
|  | * Procédez-vous à l'enregistrement et à l'analyse des incidents informatiques, notamment sur les données personnelles ? |  |  |  |
|  | * Avez-vous mis en place un registre des failles de sécurité subies par votre système d’information ? |  |  |  |
|  | * Existe-t-il une procédure de remontée d'alerte formalisée vers vos Clients en cas d'incident sur leurs données personnelles ? |  |  |  |
| ***Audit*** | * Votre société fait-elle l'objet d'audits périodiques sur les problématiques de sécurité de l'information et de protection des données personnelles ? |  |  |  |
| ***Audits techniques*** | Réalisez-vous périodiquement des tests de détection des intrusions dans vos systèmes ?  Quelle est la fréquence ? |  |  |  |
| ***Gestion de vos prestataires*** | * Les contrats avec d'autres Tiers qui peuvent potentiellement avoir accès à nos données intègrent-ils des obligations de protection des données personnelles ? |  |  |  |
| ***Gestion des traceurs*** | * Votre société respecte les lignes directrices et la recommandation de la CNIL sur le recueil d’un consentement valide de l’utilisateur de votre plateforme ? |  |  |  |