**QUESTIONNAIRE RGPD**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dénomination sociale |  | | | |
| N° SIRET |  | | | |
| Description des activités de votre société |  | | | |
| Description des prestations réalisées pour notre organisme |  | | | |
| Lieu de localisation de vos serveurs ou centres informatiques |  | Si localisation hors Union Européenne, préciser le pays : | |  |
| Lieu d’exécution de la prestation |  | Si localisation hors Union Européenne, préciser le pays : | |  |
| **Mesures techniques et organisationnelles pour garantir la sécurité physique et logique des données** | | | **Réponse**  **(oui/non)** | **Commentaire**  **(obligatoire si partiel**  **ou en projet)** |
| **Politique**  **de sécurité** | **1.**Disposez-vous d’une politique de sécurité des systèmes d’information (PSSI) ? | |  |  |
| **2.**Avez-vous désigné un responsable de la sécurité de votre système d’information (RSSI) ? | |  |  |
| **3.**Avez-vous mis en œuvre un Système de Management de la Sécurité de l’Information ou êtes-vous certifié ISO 27001 ? | |  |  |
| **4.**Avez-vous mis en œuvre un programme (ou des actions) de sensibilisation ou d’éducation à la sécurité informatique pour vos utilisateurs ? | |  |  |
| **5.**Avez-vous un système de contrôle d’accès à vos locaux ? | |  |  |
| **Données personnelles** | **6.**Avez-vous désigné un **DPO** (ou une personne responsable de la mise en conformité « protection des données à caractère personnel ») ? | |  |  |
| **7.**Avez-vous un **registre** de vos traitements de données personnelles ? | |  |  |
| **8.**Avez-vous mis en œuvre un programme de formation et sensibilisation de vos collaborateurs concernant la protection des données personnelles ? | |  |  |
| **9.**Votre personnel est-il soumis à une obligation de confidentialité ? | |  |  |
| **10.**Votre société est-elle certifiée ou labellisée sur laprotection des données à caractère personnel ? | |  |  |
| **11.**Le produit ou service fourni à notre société a-t-il fait l’objet d’une analyse d’impact sur la protection des données ? | |  |  |
| **12.**Appliquez-vous une politique de protection des données à caractère personnel ? | |  |  |
| **Confidentialité**  **des données** | **13.**Avez-vous formalisé une politique de chiffrement des données de vos Clients (en transit ou sur supports amovibles) ? | |  |  |
| **14.**Disposez-vous de solutions pour échanger de façon sécurisée des données personnelles ou sensibles avec des tiers ? | |  |  |
| **15.**Avez-vous mis en place des mesures pour limiter les habilitations de votre personnel concernant l’accès aux données de vos clients ? | |  |  |
| **Réversibilité** | **16.**Les modalités et durées de conservation des données de vos clients sont-elles définies ? | |  |  |
| **17.**Les modalités de destruction des données en fin de contrat (attestation…) sont-elles définies ? | |  |  |
| **Gestion des**  **sous-traitants** | **18.**Ferez-vous appel à une autre société pour la réalisation de la prestation pour notre organisme ? Si oui, préciser sa dénomination, son n° SIRET et sa localisation. | |  |  |
| *A compléter si vous avez répondu « oui » à la question 18:*  **19.**Le contrat avec cette autre société qui peut potentiellement avoir accès à nos données intègre-t-il des obligations de protection des données personnelles ? | |  |  |
| *A compléter si vous avez répondu « oui » à la question 18:*  **20.**Avez-vous mis en œuvre un contrôle des obligations de cette société ? | |  |  |
| **Gestion des incidents** | | | **Réponse**  **(oui/non)** | **Commentaire**  **(obligatoire si partiel**  **ou en projet)** |
| **Incident/Faille**  **de sécurité** | **21.**Avez-vousune procédure formalisée sur la gestion des incidents (détection, enregistrement, conduite à tenir communiquée au personnel, analyse, plan d’action, recensement dans une base,…) ? | |  |  |
| **22.**Avez-vous uneprocédure de remontée d’alerte formalisée vers vos Clients en cas d’incident sur leurs données personnelles ? | |  |  |
| **Audit et contrôle** | | | **Réponse**  **(oui/non)** | **Commentaire**  **(obligatoire si partiel**  **ou en projet)** |
| **Contrôle** | **23.**Votre société dispose-t-elle d’un contrôle interne qui adresse les problématiques de sécurité de l’information et de protection des données personnelles ? | |  |  |
| **Audit** | **24.**Votre société fait-elle l’objet d’audits périodiques sur les problématiques de sécurité de l’information et de protection des données personnelles ? | |  |  |
| **Audit**  **technique** | **25.**Réalisez-vous périodiquement des tests de détection des intrusions dans vos systèmes ? | |  |  |
| Souhaitez-vous ajouter d’autre(s) élément(s) autour de la sécurité ou protection des données personnelles pouvant nous intéresser et permettant de démontrer votre conformité au RGPD ? | | |  | |

Je déclare sur l’honneur que toutes les informations contenues dans ce formulaire sont exactes.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Nom et prénom** | **Fonction** | **Signature** |
|  |  |  |  |