**Annexe relative à la protection des données à caractère personnel – RGPD :** *Description des mesures de sécurité mises en œuvre*

|  |  |  |  |
| --- | --- | --- | --- |
| N° | QUESTION | REPONSE  (OUI/NON) | PIECES JOINTES |
|  | Avez-vous désigné un DPO ? |  |  |
|  | Les personnes susceptibles de consulter et d’exploiter les Données à Caractère Personnel traitées pour notre compte sont-elles sensibilisées à la protection des données ? |  |  |
|  | Les documents papiers sont-ils systématiquement conservés dans des armoires fermées à clé ? |  |  |
|  | Procédez-vous à la transmission des documents de manière sécurisée (chiffrement des documents qui présentent une certaine sensibilité, transmission des documents via des plateformes d’échange sécurisées) ? |  |  |
|  | Avez-vous une charte informatique ayant force contraignante ? |  |  |
|  | Les identifiants (login) sont-ils uniques à chaque utilisateur ? |  |  |
|  | Avez-vous une politique de gestion des mots de passe utilisateur ? |  |  |
|  | Avez-vous une politique en matière de gestion des habilitations ? |  |  |
|  | Avez-vous mis en place un process permettant de supprimer les permissions d’accès lorsqu’elles sont devenues obsolètes ? |  |  |
|  | Procédez-vous à une revue annuelle des habilitations ? |  |  |
|  | Avez-vous mis en place un système de journalisation des Données à Caractère Personnel ? |  |  |
|  | Avez-vous une procédure pour les notifications de violation de Données à Caractère Personnel ? |  |  |
|  | Avez-vous mis en place une procédure de verrouillage automatique des sessions ? |  |  |
|  | Les antivirus sont-ils régulièrement mis à jour ? |  |  |
|  | Disposez-vous de « Pare-feu » (firewall) ? |  |  |
|  | Procédez-vous à des sauvegardes ou synchronisations régulières des Données à Caractère Personnel ? |  |  |
|  | Procédez-vous à la limitation des flux réseau au strict nécessaire ? |  |  |
|  | Assurez-vous une limitation de l’accès aux outils et interfaces d’administration aux seules personnes habilitées ? |  |  |
|  | Procédez-vous à l’installation sans délai des mises à jour critiques ? |  |  |
|  | Utilisez-vous le protocole TLS ? |  |  |
|  | Procédez-vous au stockage des supports de sauvegarde dans un endroit sûr ? |  |  |
|  | Procédez-vous régulièrement à des tests de continuité d'activité ? |  |  |
|  | Avez-vous mis en en œuvre des modalités d’accès spécifiques aux données archivées ? |  |  |
|  | Détruisez-vous les archives obsolètes de manière sécurisée ? |  |  |
|  | Procédez-vous systématiquement à l’enregistrement des interventions de maintenance dans une main courante ? |  |  |
|  | Procédez-vous systématiquement à l’encadrement des interventions par des tiers ? |  |  |
|  | Procédez-vous systématiquement à l’effacement des données de tout matériel avant sa mise au rebut ? |  |  |
|  | Avez-vous mis en place des alarmes anti-intrusion ? |  |  |
|  | Mettez-vous en place systématiquement les paramétrages les plus respectueux de la vie privée des Personnes concernées ? |  |  |
|  | Procédez-vous à des tests uniquement sur des données fictives ou anonymisées ? |  |  |
|  | Avez-vous mis en place une procédure d’évaluation de vos Sous-Traitants ? |  |  |
|  | Réalisez-vous des audits réguliers de vos Sous-Traitants ? |  |  |
|  | Dans le cas du transfert de données à caractère personnel en dehors de l’UE, quelles sont les garanties mises en place pour encadrer le transfert de données ? Vers quel pays sont transférées les données personnelles ? |  |  |
|  | Autre : à préciser éventuellement |  |  |