**ANNEXE 6 : EVALUER SON NIVEAU DE MATURITE**

En ce qui concerne les réponses, celles-ci peuvent être simplement oui/non, ou plus détaillées en fonction des éléments déjà mis en place.

En ce qui concerne le niveau de maturité, celui peut s’évaluer de 1 à 4 en prenant en référence :

1 : A faire / 2 : En cours / 3 : Avancé / 4 : Terminé

Bien entendu, une autre évaluation est possible.

\* \* \*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **THEMES** | **QUESTIONS** | **NUMEROS** | **REPONSES** | **NIVEAU DE MATURITE** |
| Délégué à la protection des données (DPO) | Avez-vous nommé un délégué à la protection des données personnelles (DPO) ? Si non, avez-vous vérifié et documenté que vous n'êtes pas soumis à cette exigence? | 1 |  |  |
| Le rattachement hiérarchique du délégué à la protection des données personnelles (DPO) garantit-il son indépendance ? | 2 |  |  |
| Sous-traitants | Avez-vous identifié les sous-traitants traitant vos données personnelles ?Si oui, vous assurez vous que les sous-traitants existants et futurs sont conformes aux exigences du RGPD contractuellement et par le biais de contrôles ? | 3 |  |  |
| Avez-vous défini contractuellement des exigences en termes de protection des données avec vos sous-traitants informatiques (prestataires ou fournisseurs) ? | 4 |  |  |
| Effectuez-vous régulièrement des contrôles / audit de sécurité de vos sous-traitants informatiques (prestataires ou fournisseurs) ? | 5 |  |  |
| Registre des traitements | Avez-vous identifié pour vos traitements : les finalités, les personnes concernées, les catégories de données traitées ? | 6 |  |  |
| Avez-vous établi un registre des traitements dont vous êtes responsable, co-responsable ou sous-traitant? | 7 |  |  |
| Avez-vous une cartographie exhaustive des données personnelles traitées dans votre système d'information ? | 8 |  |  |
| Pour les traitements soumis à des hauts risques potentiels sur la vie privée, avez-vous consulté le DPO et vérifié le respect des conditions spécifiques ? | 9 |  |  |
| Licéité | Pouvez-vous justifier la base légale de chacun de vos traitements ? | 10 |  |  |
| Lorsque la base légale du traitement est le consentement, avez-vous mis en place des mécanismes de gestion de ces consentements? | 11 |  |  |
| Si vous collectez des catégories particulières de données (données sensibles), avez-vous vérifié la licéité de leur collecte et de leur traitement? | 12 |  |  |
| Minimisation | Avez-vous vérifié la proportionnalité des données collectées aux finalités des traitements ? | 13 |  |  |
| Durée de conservation | Des durées de conservation sont-elles définies pour les données traitées ?Si oui, les durées sont-elles communiquées aux personnes concernées ? | 14 |  |  |
| Information des personnes concernées | Les personnes concernées bénéficient-elles d’une information claire et compréhensible lors de la collecte des données ?  | 15 |  |  |
| Droit des personnes | Avez-vous une procédure validée et testée pour répondre aux demandes d’exercice des droits prévus par le RGPD : droits d'accès, de rectification, de suppression des données de droit à l'oubli, de droit à la portabilité ou de limitation de traitement ? | 16 |  |  |
| Avez-vous défini et mis en œuvre une ou des solutions pour répondre aux demandes d’accès, de rectification, de suppression des données, de droit à l'oubli, de droit à la portabilité, de limitation des traitements dans vos applications ? | 17 |  |  |
| Transferts | Si vous effectuez des transferts de données personnelles à des partenaires situés hors de l’Union Européenne, vous êtes-vous rapprochés de votre DPO ou de votre service juridique pour vérifier que les transferts effectués soient couverts par des garanties appropriées ?  | 18 |  |  |
| Analyses d’impact | Avez-vous défini des critères de décision pour déterminer si une Etude d'impact sur la vie privée était nécessaire ? | 19 |  |  |
| Si la criticité du traitement implique une étude d'impact sur la vie privée (DPIA), avez-vous effectué cette étude en coordination avec DPO ?  | 20 |  |  |
| Avez-vous défini une méthode d'étude d'impact vie privée en coordination avec le DPO ?  | 21 |  |  |
| Notification des violations des données | Avez-vous établi la procédure de détection, de traitement et de notification des violations de données personnelles ? | 22 |  |  |
| Sécurité | Avez-vous mis en place des mécanismes de protection des données personnelles (notamment chiffrement ou de pseudonymisation) ? | 23 |  |  |
| Avez-vous  défini et mis en place des mesures de sécurisation des accès administrateurs privilégiés ? | 24 |  |  |
| Avez-vous intégré les éléments de conformité au RGPD dans votre politique de sécurité des systèmes d'information et dans votre charte informatique ? | 25 |  |  |
| Avez-vous défini et mis en place des procédures de gestion des accès aux systèmes contenant de données personnelles ?  | 26 |  |  |
| Avez-vous mis en place des mécanismes d'archivage et de suppression des données personnelles ? | 27 |  |  |
| Documentation | Avez-vous intégré les éléments de conformité au RGPD dans vos politiques et procédures ? | 28 |  |  |
| Une veille juridique a-t-elle été mise en place pour suivre les évolutions réglementaires ? | 29 |  |  |
| Formation | Les politiques et procédures en lien avec le RGPD sont-elles diffusées aux collaborateurs de votre SSTI ? | 30 |  |  |
| Avez-vous intégré le RGPD à votre programme de formation RH ? | 31 |  |  |
| Assurance | Avez-vous revu la couverture d’assurance de votre SSTI pour tenir en compte du RGPD ? | 32 |  |  |