**Check-list « gouvernance »**

| Sous thème | # | Question | Commentaire / Exemple |
|---|---|---|---|
| **DPO (délégué à la protection des données personnelles)** | **1** | Avez-vous nommé DPO ? Si non, avez-vous vérifié et documenté que vous n'êtes pas soumis à cette exigence ? | D'après l'article 37 §1, la nomination d'un DPO est notamment obligatoire dans le cas où vos activités de base consistent des opérations de traitement à grande échelle impliquant un suivi systématique des personnes concernées, ou des données sensibles au sens des articles 9 et 10. |
| | **2** | Le rattachement hiérarchique du délégué à la protection des données personnelles (DPO) garantit-il son indépendance ? | |
| **Périmètre d'application** | **3** | Avez-vous déterminé le périmètre des entités / Business Unit concernées par le plan de mise en conformité ? | |
| | **4** | Avez-vous établi un registre des traitements dont vous êtes responsable, co-responsable ou sous-traitant ? | Le registre comporte le nom et les coordonnées du responsable du traitement, les finalités du traitement, les catégories de destinataires et des personnes concernées, etc. |
| | **5** | Avez-vous identifié les transferts de données personnelles hors Union Européenne ? Si oui, avez-vous formalisé les garanties mises en œuvre ou à l'étude ? | Garanties cf. chapitre V du GDPR : soit niveau de protection adéquate du pays tiers (art. 44) soit mécanisme de sauvegarde visé à l'art 46 (par ex. Binding Corporate Rules) |
| | **6** | Avez-vous réalisé un état des lieux des processus métiers traitant des données personnelles ? | |
| | 7 | Avez-vous identifié les sous-traitants traitant vos données personnelles ?<br>Si oui, vous assurez-vous que les sous-traitants existants et futurs sont conformes aux exigences du GDPR contractuellement et par le biais de contrôles ? | |
| **Mise en conformité** | **8** | Avez-vous mis en place une organisation projet pour la mise en conformité au GDPR ? | Une organisation projet couvre généralement le(s) sponsor(s), l'équipe projet, les tâches, jalons et livrables |

| Sous thème | # | Question | Commentaire / Exemple |
|---|---|---|---|
| | **9** | Avez-vous établi une feuille de route pour la mise en conformité au GDPR ? | Une feuille de route propose généralement les projets, le recensement des moyens, la cible à atteindre, la priorité des tâches, ainsi qu'un calendrier pour atteindre ces buts. |
| | **10** | Existe-t-il un reporting périodique au Board/Comex pour s'assurer de l'avancement du plan d'action et décider d'actions correctrices ? | |
| | **11** | Le plan d'audit intègre-t-il des missions de contrôle de la mise en conformité au GDPR ? | |
| **Politiques et procédures** | **12** | Avez-vous intégré les éléments de conformité au GDPR dans vos politiques et procédures ? | Les politiques précisent les durées de conservation des données personnelles, la sécurité des données, la suppression des données, la notification en cas de violation des données personnelles, la validation périodique de la pertinence du dispositif en place, etc. |
| **Veille juridique** | **13** | Une veille juridique a-t-elle été mise en place pour suivre les évolutions réglementaires ? | Exemple : guidelines émises par le G29 (WP29) |
| **Formation** | **14** | Les politiques et procédures en lien avec le GDPR sont-elles diffusées aux collaborateurs de votre entreprise ? | Exemple : code de conduite |
| | **15** | Avez-vous intégré le GDPR à votre programme de formation RH ? | Le programme de formation inclut des dispositifs comme du E-learning, des formations régulières (Manager, SI, métiers), des actions de communication, etc. |
| **Assurance** | **16** | Avez-vous revu la couverture d'assurance de votre entreprise pour tenir en compte du GDPR ? | |

**Check-list « Métiers »**

| Sous thème | # | Question | Commentaire / Exemple |
|---|---|---|---|
| **Licéité des traitements** | **17** | Avez-vous identifié pour vos traitements les finalités, les personnes concernées et les catégories de données traitées ? | Ces éléments sont un préalable nécessaire à l'établissement du registre de traitements exigé par le GDPR pour chaque responsable de traitement et sous-traitant. |
| | **18** | Avez-vous vérifié la proportionnalité des données collectées aux finalités des traitements ? | Limiter par défaut le traitement de données à caractère personnel à ce qui est strictement nécessaire, en ce qui concerne la quantité de données traitées, leur accessibilité et leur période de conservation. |
| | **19** | Pouvez-vous justifier la base légale de chacun de vos traitements ? | Le traitement doit être fondé sur une base légale prévue à l'article 6 du GDPR (licéité), qui peut être : une obligation légale, l'intérêt légitime du responsable de traitement, l'exécution d'un contrat, le consentement exprimé par la personne concernée, la protection des intérêts vitaux d'une personne concernée, une mission d'intérêt ou de service public. |
| | **20** | Lorsque la base légale du traitement est le consentement, avez-vous mis en place des mécanismes de gestion de ce consentement ? | Gestion : recueil, enregistrement, modification, révocation, etc. |
| | **21** | Pour les traitements impliquant le croisement entre plusieurs catégories de données (interconnexion de fichiers), la réutilisation de données collectées lors d'un autre traitement ou l'enrichissement des données, avez-vous consulté le DPO et vérifié la conformité au GDPR ? | Si vous<br>- effectuez des croisements entre plusieurs catégories de données collectées séparément, ou<br>- réutilisez des données collectées pour un autre traitement, ou<br>- utilisez des données fournies par une tierce partie,<br>Vous devez vérifier que votre traitement est conforme aux finalités pour lesquelles les données ont été collectées ou, le cas échéant, aux consentements donnés par les personnes concernées |
| | **22** | Des durées de conservation sont-elles définies pour les données traitées ?<br>Si oui, les durées sont-elles communiquées aux personnes concernées ? | |

| Sous thème | # | Question | Commentaire / Exemple |
|---|---|---|---|
| **Types de traitements** | **23** | Pour les traitements entrant dans le cadre du profilage, avez-vous consulté le DPO et vérifié la conformité au GDPR ? | Profilage : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique |
| | **24** | 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 ? | Exemples de traitement : vidéosurveillance, géolocalisation, whistleblowing, écoute sur le lieu de travail, contrôle d'accès aux locaux, biométrie, etc. |
| **Catégories des données collectées** | **25** | Si vous collectez des catégories particulières de données (données sensibles), avez-vous vérifié la licéité de leur collecte et de leur traitement ? | Cf. articles 9 et 10 du GDPR. |
| **Droits des personnes** | **26** | Les personnes concernées bénéficient-elles d'une information claire et compréhensible lors de la collecte des données ? | |
| | **27** | Avez-vous une procédure validée et testée pour répondre aux demandes d'exercice des droits prévus par le GDPR ?<br><br>En particulier droits d'accès, de rectification, de suppression des données de droit à l'oubli, de droit à la portabilité ou de limitation de traitement ? | Y compris la notification des demandes de rectification ou de suppression aux sous-traitants ou autres tierces parties destinataires des données. |
| | **28** | Les personnes concernées peuvent-elles modifier leur consentement ? | Exemple : Self-service. |
| **Contractualisation avec les sous-traitants** | **29** | Avez-vous défini contractuellement avec vos sous-traitants des exigences en termes de protection des données ? | |
| **Transferts de données en dehors de l'Espace Economique Européen** | **30** | Si vous effectuez des transferts de données personnelles à des entreprises situées 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 ? | |
| **Sécurité des données personnelles** | **31** | Avez-vous exprimé des exigences de protection des données personnelles vis à vis de votre service informatique ? | Exemple d'exigences de sécurité : pseudonymisation, chiffrement, stockage et transferts sécurisés, règles de purge ou d'archivage, etc. |

| Sous thème | # | Question | Commentaire / Exemple |
|---|---|---|---|
| | **32** | Etes-vous associé au processus de détection, de traitement et de notification des violations de données personnelles ? | |
| **Etude d'impact sur la vie privée (DPIA)** | **33** | Avez-vous défini des critères de décision pour déterminer si une Etude d'impact sur la vie privée (DPIA) était nécessaire ? | |
| | **34** | Si la criticité du traitement implique une étude d'impact sur la vie privée (DPIA), avez-vous effectué cette étude en coordination avec le DPO ? | |

## Check-list « Systèmes d'Information et cybersécurité »

| Sous thème | # | Question | Commentaire / Exemple |
|---|---|---|---|
| **Cartographie des systèmes d'informations (SI)** | **35** | Avez-vous une cartographie exhaustive des données personnelles traitées dans votre système d'information ? | Dictionnaire de données, accès (utilisateurs, interfaces), applications, bases de données, serveurs, Datacenter, services cloud, localisation, etc. |
| **Sécurité des données personnelles** | **36** | Avez-vous intégré les éléments de conformité au GDPR dans votre politique de sécurité des systèmes d'information ? | |
| | **37** | Utilisez-vous des standards ou des guides de bonnes pratiques Security by design ? | Exemples de référentiels de sécurité : ISO27001, NIST, guide d'hygiène ANSSI, CIS critical security controls, etc. |
| | **38** | Avez-vous défini et mis en place des procédures de gestion des accès aux systèmes contenant des données personnelles ? | Conception des habilitations, ajout/suppression des droits, revues régulières des droits d'accès) |
| | **39** | Avez-vous défini et mis en place des mesures de sécurisation des accès administrateurs privilégiés ? | Bastion, enregistrement de sessions des comptes à privilèges sur les serveurs, ...) |
| | **40** | Avez-vous mis en place des mécanismes de protection des données personnelles (notamment chiffrement ou de pseudonymisation) ? | Données stockées sur les serveurs (Data at Rest) et pour le transport de ces données sur le réseau (Data in transit), (exemples : outils de tokenisation, ...) |

| Sous thème | # | Question | Commentaire / Exemple |
|---|---|---|---|
| **Protection de la vie privée dès la conception (« privacy by design »)** | **41** | Avez-vous mis en place des mécanismes d'archivage et de suppression des données personnelles ? | |
| | **42** | Ces mécanismes sont-ils alignés sur la politique de conservation (notamment avec les durées légales ou contractuelles de rétention des données) ? | |
| | **43** | Avez-vous mis en place des mécanismes permettant d'isoler les environnements de production et de non production (test, recette) ? | Segmentation réseau, pare feux, anonymisation éventuelle des données personnelles en environnements de non production. |
| **Transparence, information** | **44** | Avez-vous mis en place des mécanismes de traçabilité et de détection d'accès aux données personnelles ? (Notamment déplacement ou copie de données non autorisés déclenchant des alertes aux équipes sécurité) | Accès des utilisateurs/interfaces, déplacements et copies en masse des données à personnelles, etc. |
| **Dispositif de détection et de notification** | **45** | Avez-vous établi la procédure de détection, de traitement et de notification des violations de données personnelles ? | Procédure détaillant la détection, la réponse à incident et la communication en cellule de crise, puis l'autorité dans les 72 heures |
| **Contractualisation avec les sous-traitants** | **46** | Avez-vous défini contractuellement des exigences en termes de protection des données avec vos sous-traitants informatiques (prestataires ou fournisseurs) ? | Exemples : questionnaire de sécurité, clauses contractuelles liées à la protection des données, clause d'audit de sécurité, suppression des données à la fin de la prestation, etc. |
| **Codes de conduite et Certification** | **47** | Effectuez-vous régulièrement des contrôles / audit de sécurité de vos sous-traitants informatiques (prestataires ou fournisseurs) ? | Exemples : vérification de la mise en place des clauses de sécurité, audit technique de sécurité, tests d'intrusion, etc. |
| **Etude d'impact sur la vie privée (DPIA)** | **48** | Avez-vous défini des critères de décision pour déterminer si une Etude d'impact sur la vie privée (DPIA) était nécessaire ? | |
| | **49** | Avez-vous défini une méthode d'étude d'impact vie privée en coordination avec le DPO ? | Exemples : Etude d'impacts sur la vie privée : la méthode de la CNIL |
| **Gestion de l'exercice des droits des personnes** | **50** | Avez-vous défini et mis en œuvre une ou plusieurs 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 ? | Sauf exception, le GDPR impose un délai maximum d'un mois pour répondre aux demandes d'exercice de leurs droits par les personnes concernées (Art. 12.3). |