Vienne Condrieu Agglomération

# PLAN D'ACTION DE MISE EN CONFORMITE RGPD AVEC IDENTIFICATION DES PRIORITES

| Département responsable | Stream | Actions | Catégorie de livrable | Explication | Priorité | Hypothèses de travail | Date de début | Date de fin |
|---|---|---|---|---|---|---|---|---|
| DGS | 1 - Gouvernance et accountability | Validation du programme de mise en conformité indiquant les actions par ordre de priorité, le budget, les échéances et un RACI. | Programme de mise en conformité | Le programme de mise en conformité, les feuilles de route et le chiffrage associé établis par DPO Consulting doivent être validés par la Direction. | 1 | Validation du programme de mise en conformité en Conseil d'administration (date à ajuster) : Réunion de travail pour valider les actions et voter le budget | 01/04/2023 | 01/07/2023 |
| DPO | 6 - Information aux personnes concernées | Créer des mentions d'information (conformes au RGPD) afin d'informer les personnes concernées des traitements qui sont réalisés avec leurs données personnelles. Exemples : -Clause RGPD à destination des collaborateurs (ex: notice d'information RGPD envoyée avec les fiches de paie) ; -Formulaire de demande de composteur | Templates mentions d'information | Toute personne dont les données à caractère personnel font l'objet d'un traitement doivent recevoir de la part du Responsable de traitement les informations listées à l'article 13 du RGPD (ou article 14 en cas de collecte indirecte). | 1 | Rédaction des mentions d'information sur les différents supports collecteurs de données | 01/04/2023 | 01/07/2023 |
| DPO | 6 - Information aux personnes concernées | Créer/Mettre à jour des/les mentions d'information (conformes au RGPD) pour les formulaires de recueil de consentement (ex : formulaire de consentement pour la collecte et la diffusion des photographies des personnes concernées) | Templates mentions d'information | Toute personne dont les données à caractère personnel font l'objet d'un traitement doivent recevoir de la part du Responsable de traitement les informations listées à l'article 13 du RGPD (ou article 14 en cas de collecte indirecte).<br>De plus, il conviendra de veiller à ce que le consentement soit recueilli le manière libre, spécifique, éclairé et univoque.<br>Enfin, il sera nécessaire d'informer les personnes concernées des modalités mises en place pour permettre le retrait de consentement de la personne concernée. | 1 | Rédaction de mentions d'information sur les différents supports relatifs aux consentements | 01/04/2023 | 01/07/2023 |
| Service informatique | 6 - Information aux personnes concernées | Compléter la politique de confidentialité du site internet de Vienne Condrieu Agglomération | Politique | La politique doit contenir les mentions suivantes :<br>- identité et coordonnées du responsable du traitement<br>- Le détail des données collectées (ex : nom, prénom, date de naissance, etc.)<br>- L'utilisation des données personnelles: identification de toutes les finalités (cf. Cartographie des traitements)<br>- La durée de conservation des données pour chaque finalité<br>- L'existence de partage de données personnelles avec des tiers<br>- L'existence ou non de transferts de données personnelles et si oui, dans quelles conditions<br>- Les mesures de sécurité et confidentialité<br>- Les droits des personnes concernés quant à leurs données | 1 | - Rédaction d'une document d'une dizaine de pages.(inclure une partie relative à l'utilisation des cookies ou intégrer dans un onglet différent une politique cookies)<br><br>- Implémentation dans un endroit dédié sur le site internet de l'agglomération | 01/04/2023 | 01/07/2023 |
| Service informatique | 6 - Information aux personnes concernées | Compléter la politique cookies pour le site internet de Vienne Condrieu Agglomération (mention d 'une utilisation des cookies de la suite Google Analytics malgré l'interdiction de la CNIL et information différentes entre la politique cookies et le bandeau cookies) + Supprimer les cookies de la Suite Google Analytics + indiquer dans l'onglet concerné en bas de page qu'il renvoi à des informations relatives à la gestion des données personnelles (politique de confidentialité) et la gestion des cookies informatiques | Politique | Par défaut, le consentement pour tout type de cookies ne pourra être activé. Il appartiendra à l'utilisateur de les accepter de manière libre, éclairé, spécifique et univoque.<br>Le politique cookies doit contenir les mentions d'information suivantes à son affichage :<br>- identité et coordonnées du responsable du traitement<br>- Le détail des données collectées (ex : nom, prénom, date de naissance, etc.)<br>- L'utilisation des données personnelles: identification de toutes les finalités (cf. Cartographie des traitements)<br>- La durée de conservation des données pour chaque finalité<br>- L'existence de partage de données personnelles avec des tiers<br>- L'existence ou non de transferts de données personnelles et si oui, dans quelles conditions<br>- Les mesures de sécurité et confidentialité<br>- Les droits des personnes concernés quant à leurs données | 1 | - Mise à jour de la politique cookies<br><br>- Implémentation dans un endroit dédié sur le sites internet (expression de besoin) ;<br><br>- Module de gestion du consentement permettant à l'utilisateur de donner ou de retirer son consentement au recours aux cookies à tout moment. | 01/04/2023 | 01/07/2023 |

Priorité 1

| Département responsable | Stream | Actions | Catégorie de livrable | Explication | Priorité | Hypothèses de travail | Date de début | Date de fin |
|---|---|---|---|---|---|---|---|---|
| **DPO** | 9 - Analyse d'impact sur la vie privée | Mettre en place une méthode d'analyse d'impact sur la vie privée (AIPD) | Procédure | Pour les traitements à risque (traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées), le RGPD impose la réalisation d'AIPD | 1 | Document de 5-15 pages prenant appui sur les guides et recommandations de la CNIL, et formalisant l'usage de l'outil PIA développé par la CNIL. La méthode doit comprendre a minima :<br>- une grille d'évaluation des risques permettant de déterminer si une analyse d'impact est requise ;<br>- un RACI de la gouvernance des analyses d'impact ;<br>- un processus de consultation obligatoire et de validation du DPO ;<br>- les hypothèses de consultation de la CNIL préalablement à la mise en œuvre du traitement. | 01/04/2023 | 01/07/2023 |
| **DPO** | 9 - Analyse d'impact sur la vie privée | Réalisation du PIA (RACI sur la base de la réalisation d'un PIA) concernant la mise en place de caméras de vidéoprotection | Etude de risque | Identifier les traitements à risque | 1 | Consulter les documents de références pour déterminer les traitements nécessitant une analyse d'impact et ceux dispensés. Identifier les traitements à risque et leur appliquer la méthode d'AIPD | 01/04/2023 | 01/07/2023 |
| **DPO** | 12 - Sous-traitants | Etablir une grille d'évaluation de la conformité des sous-traitants avant la sélection ainsi qu'une grille interne des actions à entreprendre pour les sélectionner. | Grille d'évaluation des sous-traitants | Le questionnaire est basé sur les obligations contractuelles que vous imposez aux sous-traitants dans le cadre de vos propres clauses/checklists. Il comprend les exigences RGPD, les exigences sécurité et un score que vous attribuerez en fonction des réponses données. | 1 | Document Checklist de 2 pages. | 01/04/2023 | 01/07/2023 |
| **DPO** | 12 - Sous-traitants | Mettre en place et négocier des avenants/contrats pour les prestataires/contrats ayant le statut de sous-traitant en matière de données personnelles. | Clauses contractuelles | Le responsable de traitement doit sécuriser les relations contractuelles établies avec ses sous-traitants. | 1 | Etablir des modèles de clauses de protection des données personnelles en fonction du degré de risque estimé. | 01/04/2023 | 01/07/2023 |
| **Service informatique** | 14 - Notification des failles de sécurité | Mettre en place une procédure de gestion des violations de données | Procédure | Tout incident de sécurité (numérique, physique, matériel, organisationnel, humain) est susceptible d'engendrer une violation de données personnelles.<br>Le responsable de traitement doit être en mesure d'identifier les cas dans lesquels un incident de sécurité engendre une violation de données personnelles. | 1 | Document de 5-10 pages comprenant notamment:<br>- Critères et méthode permettant de déterminer si un faille de sécurité engendre une violation de données personnelles ;<br>- Critères et méthode d'évaluation des risques ou conséquences potentielles de la violation ;<br>- Répartition et description des rôles de chaque personne contributrice ;<br>- Implications éventuelles de tiers (prestataires, partenaires, etc.) dans l'origine ou la gestion d'une violation ;<br>- Critères de déclenchement d'une notification à la CNIL et, le cas échéant, aux personnes concernées. | 01/04/2023 | 01/07/2023 |

| Département responsable | Stream | Actions | Catégorie de livrable | Explication | Priorité | Hypothèses de travail | Date de début | Date de fin |
|---|---|---|---|---|---|---|---|---|
| **DPO** | 1 - Gouvernance et accountability | Etablir une politique générale de protection des données. | Politique Générale de protection des données | La politique présente :<br>• les principes de protection des données à respecter par tous les collaborateurs ;<br>• les exigences complémentaires en cas de collecte et traitement de données dites sensibles ;<br>• les exigences complémentaires relatives au consentement comme base légale ;<br>• les modalités d'encadrement des tiers intervenant sur tout ou partie d'un traitement ;<br>• le modèle de gouvernance autour de la protection des données personnelles, avec identification des compétences clés en interne et leurs rôles et responsabilités ;<br>• les relations avec l'autorité de contrôle ;<br>• les modalités de contrôle du respect, en interne, des exigences du RGPD. | 2 | Document 15-20 pages récapitulant les points listés dans les explications. | 01/07/2023 | 01/10/2023 |
| **Ressources humaines** | 1 - Gouvernance et accountability | Communiquer la politique à l'ensemble des collaborateurs et la mettre à disposition dans un endroit facilement accessible. | Communication | Plan de communication une fois que la politique sera validée. Elle devra être communiquée à l'ensemble des collaborateurs. Il faudra choisir le canal de communication le plus adapté à la structure (E-mail, livret distribué à chaque collaborateur à son arrivée…) et en conserver les éléments de preuve. | 2 | - Réunion de sensibilisation et/ou communication électronique par email, affichage ou distribution d'un exemplaire papier pour communiquer la politique en interne.<br>- Rendre la politique pour que chacun puisse en prendre connaissance de manière simple. | 01/07/2023 | 01/10/2023 |
| **DGS** | 2 - Registre des traitements | Compléter le registre des traitements | Registre | Le registre des traitements est le document clé à présenter à la CNIL en cas de contrôle. Il doit être complété et mis à jour de façon régulière. | 2 | Compléter et valider le registre établi par DPO Consulting. | 01/07/2023 | 01/10/2023 |
| **DGS** | 3 - Formations en matière de protection des données personnelles | Définir un plan de formation/ sensibilisation en matière de données personnelles. | Formation | Définir les cibles pour les formations : liste des personnes à former, type de formation, planning en fonction des urgences et nécessités. | 2 | - Définir le mode de formation (e-learning, présentiel, etc.), définir s'il y aura recours à un prestataire externe pour établir la formation ;<br>- Recenser les collaborateurs à former, définir le calendrier et les sujets de formation puis valider. | 01/07/2023 | 01/10/2023 |
| **Ressources humaines** | 3 - Formations en matière de protection des données personnelles | Déployer le plan de formation : sensibilisation générale de tous les collaborateurs + formations spécifiques pour les collaborateurs identifiés. | Formation | Temps de formation | 2 | Déterminer le nombre de personnes par atelier, la durée des ateliers, éventuellement la méthode d'évaluation | 01/07/2023 | 01/10/2023 |

Priorité 2

| Département responsable | Stream | Actions | Catégorie de livrable | Explication | Priorité | Hypothèses de travail | Date de début | Date de fin |
|---|---|---|---|---|---|---|---|---|
| **DGS** | 4 - Délégué à la protection des données | Mettre en place une note d'organisation pour la nomination du DPO (organisation, RACI, délégation, fiche de poste).<br>Il conviendra d'indiquer les raisons pour lesquelles la désignation d'un DPO est obligatoire pour Vienne Condrieu Agglomération | Note d'organisation | Mise en place d'une fiche de poste définissant la mission du DPO | 2 | Document d'une page reprenant l'ensemble des missions principales du DPO ainsi que le moyen de contact pour communiquer avec lui | 01/07/2023 | 01/10/2023 |
| **DPO** | 5 - Licéité des traitements | Mettre en œuvre de manière opérationnelle une minimisation de la collecte de données au sein des services.<br>Il conviendra en effet de vérifier que les formulaires de collecte de données ne contiennent pas de données qui ne seraient pas réellement nécessaires pour effectuer les traitements de données en question.<br>Ex: Formulaire de contact du site internet | Action | Le principe de minimisation de la collecte de données implique de ne collecter que les données strictement nécessaires à la réalisation d'un traitement de données. (Article 5, 1, c du RGPD). | 2 | Analyser l'ensemble des formulaires de collecte de données (ex: formulaire de contact du site internet) et supprimer les données qui ne sont pas nécessaires à la réalisation des traitements de données. | 01/07/2023 | 01/10/2023 |
| **DPO** | 7 - Conservation des données | Elaborer une politique de conservation des données comprenant:<br>- le référentiel des durées de conservation ;<br>- la procédure de purge des données ;<br>- le modèle de certificat de destruction des données ;<br>- la liste des personnes qui sont responsables de la suppression ;<br>- les mesures de suppression et la communiquer aux services | Politique de conservation des données | Le RGPD impose de définir des durées de conservation pour chaque traitement identifié.<br><br>Ex :<br>- Documents comptables (livres, registres, factures, bons de commande) : 10 ans à partir de la clôture de l'exercice.<br>- Données RH relatives aux agents : d'une manière générale, les données personnelles sont conservées et traitées pendant toute la durée d'exécution de la relation de travail, et sont ensuite archivées conformément aux directives des Archives départementales.<br>- Cookies informatique : 13 mois | 2 | - Politique avec référentiel de 20/30 pages.<br>- Analyse pour chaque traitement de la durée de conservation adaptée au regard de la finalité, des obligations légales, des recommandations de la CNIL et des besoins opérationnels.<br>- Etude des possibilités techniques et opérationnelles de purge | 01/07/2023 | 01/10/2023 |
| **DPO** | 7 - Conservation des données | Suppression des données personnelles/documents papiers ou informatiques dont la durée de conservation est dépassée. Mise à jour des données inexactes | Action | Opération de tri dans chaque service pour supprimer ou mettre à jour les données personnelles détenues. | 2 | Opération de tri par les collaborateurs pour supprimer les fichiers contenant des données personnelles qui n'ont plus lieu d'être conservées. | 01/07/2023 | 01/10/2023 |

| Département responsable | Stream | Actions | Catégorie de livrable | Explication | Priorité | Hypothèses de travail | Date de début | Date de fin |
|---|---|---|---|---|---|---|---|---|
| **DPO** | 11 - Réponses aux réclamations des personnes concernées | Mettre en place une procédure de gestion des demandes des personnes concernées (opposition, rectification…). | Procédure | Le document doit comprendre :<br>- une synthèse sur les droits des personnes (accès, modification, limitation, opposition, suppression, portabilité) ;<br>- les critères d'évaluation du caractère infondé/excessif d'une demande ;<br>- des modèles de réponse. | 2 | - Rédaction du document<br>- Communication en interne<br><br>Document à annexer à la politique générale de protection des données | 01/07/2023 | 01/10/2023 |
| **Service informatique** | 13 - Sécurité des données personnelles | Rédiger une politique de sécurité des systèmes d'information (PSSI) | Politique | La politique de sécurité des systèmes d'information au regard de la sensibilité comprend :<br>• La répartition des rôles de chaque personne amenée à administrer le SI et sa fiche de poste ;<br>• Les habilitations d'accès aux bases de données indiquant les accès autorisés par catégorie de données et d'application ;<br>• Les mesures de sécurité logiques et physiques à mettre en place;<br>• Une procédure de journalisation des accès | 2 | Rédaction d'un document d'une quinzaine de pages réintégrant les éléments relatifs à la gestion des accès existants.<br><br>Communication interne à l'ensemble des collaborateurs de l'agglomération | 01/07/2023 | 01/10/2023 |
| **Service informatique** | 13 - Sécurité des données personnelles | Compléter la charte informatique avec une clause relative à la protection des données personnelles + Diffuser la charte en interne. | Politique | La charte informatique doit inclure des règles sur l'utilisation du SI, sur les bonnes pratiques de navigation, sur les risques d'infection de la messagerie, etc.<br>Les agents ont des droits et des devoirs. Le document doit rappeler que :<br>- D'une part, le responsable de traitement va traiter des données les concernant dans le cadre de la relation de travail ; les agents ont ainsi des droits en tant que personnes concernées.<br>- D'autre part, les agents vont traiter au quotidien, dans le cadre de leurs missions, les données personnelles de nombreuses personnes ; ils ont ainsi des devoirs de confidentialité et de respect des règles RGPD. | 2 | Rédaction d'un document comprenant les exigences et bonnes pratiques relatives à la protection des données personnelles, sous forme d'engagement à respecter par les collaborateurs. | 01/07/2023 | 01/10/2023 |
| **Services opérationnels** | 13 - Sécurité des données personnelles | Mise en place d'actions visant à éviter la duplication de données à des fins de sécurisation.<br>Ex: Ne pas conserver 3 fichiers Excel différents contenant quasiment les mêmes informations afin de ne pas multiplier la donnée. | Action organisationnelle | La multiplication des données peut s'avérer dangereuse d'un point de vue de la sécurité. | 2 | Rassembler les données personnelles qui peuvent l'être dans des fichiers plus complets.<br>Supprimer les fichiers devenus inutiles. | 01/07/2023 | 01/10/2023 |

Priorité 2

| Département responsable | Stream | Actions | Catégorie de livrable | Explication | Priorité | Hypothèses de travail | Date de début | Date de fin |
|---|---|---|---|---|---|---|---|---|
| **Ressources humaines** | 3 - Formations en matière de protection des données personnelles | Etablir un registre des formations pour conserver les preuves de la formation des collaborateurs (liste d'émargement, supports de formation, résultats des tests). | Registre | Le registre est nécessaire en cas de contrôle pour apporter la preuve qu'une opération de sensibilisation est en cours. | 3 | Suivi du programme des formations par le biais d'un registre Excel. | 01/10/2023 | 01/01/2024 |
| **DPO** | 11 - Réponses aux réclamations des personnes concernées | Mettre en place un registre des demandes des personnes concernées. | Registre | Les personnes concernées bénéficient d'un certain nombre de droits (accès, suppression, opposition, limitation, rectification, etc).<br>La Collectivité doit être en mesure d'y répondre et de les gérer. | 3 | Création d'un registre (format Excel). | 01/07/2023 | 01/10/2023 |
| **DPO** | 14 - Notification des failles de sécurité | Elaborer et mettre à jour un registre des violations des données personnelles. | Registre | Suivi des violations de données personnelles et de leurs détails (type de violation, date et heure, description, localisation, données affectées, catégories des personnes affectées, mesures prises avant la faille et après la faille, justification d'une absence de notification à la CNIL et/ou aux personnes etc.). | 3 | Fichier Excel | 01/07/2023 | 01/10/2023 |
| **DPO** | 15 - Relations avec l'autorité de contrôle | Elaborer un guide sur la gestion des contrôles CNIL. | Procédure | Le document explique ce qu'il faut faire et ce qu'il ne faut pas faire en cas de contrôle de la CNIL afin d'éviter un délit d'entrave à la mission de la CNIL. | 3 | Document 3-5 pages indiquant aux employés comment gérer les contrôles CNIL + communication du document à tous les agents. | 01/10/2023 | 01/01/2024 |
| **Ressources humaines** | 15 - Relations avec l'autorité de contrôle | Diffuser un guide sur la gestion des contrôles CNIL. | Communication | Communication aux collaborateurs du guide des contrôle CNIL | 3 | | 01/10/2023 | 01/01/2024 |

Priorité 3