DPO Consulting
Your personal data protection officer

# Vienne Condrieu Agglomération

## Restitution – Plan de mise en conformité initiale

02 mars 2023

Vienne Condrieu Agglomération

1. Déroulement de la mission
2. Cartographie des traitements
3. Analyse du niveau de maturité
4. SWOT - Forces / Faiblesses / Opportunités / Menaces
5. Programme de mise en conformité
6. Actions prioritaires
7. Prochaines étapes

# 1. Déroulement de la mission

# 1 Déroulement de la mission

**AUDIT des services** → **CARTOGRAPHIE des traitements** → **ANALYSE de risque** → **ANALYSE de maturité**

Situation de Vienne Condrieu Agglomération par rapport à la réglementation ?

→ **PROGRAMME DE MISE EN CONFORMITE** → **DEPLOIEMENT du programme**

# 1 Déroulement de la mission

## Entretiens à Vienne Condrieu Agglomération

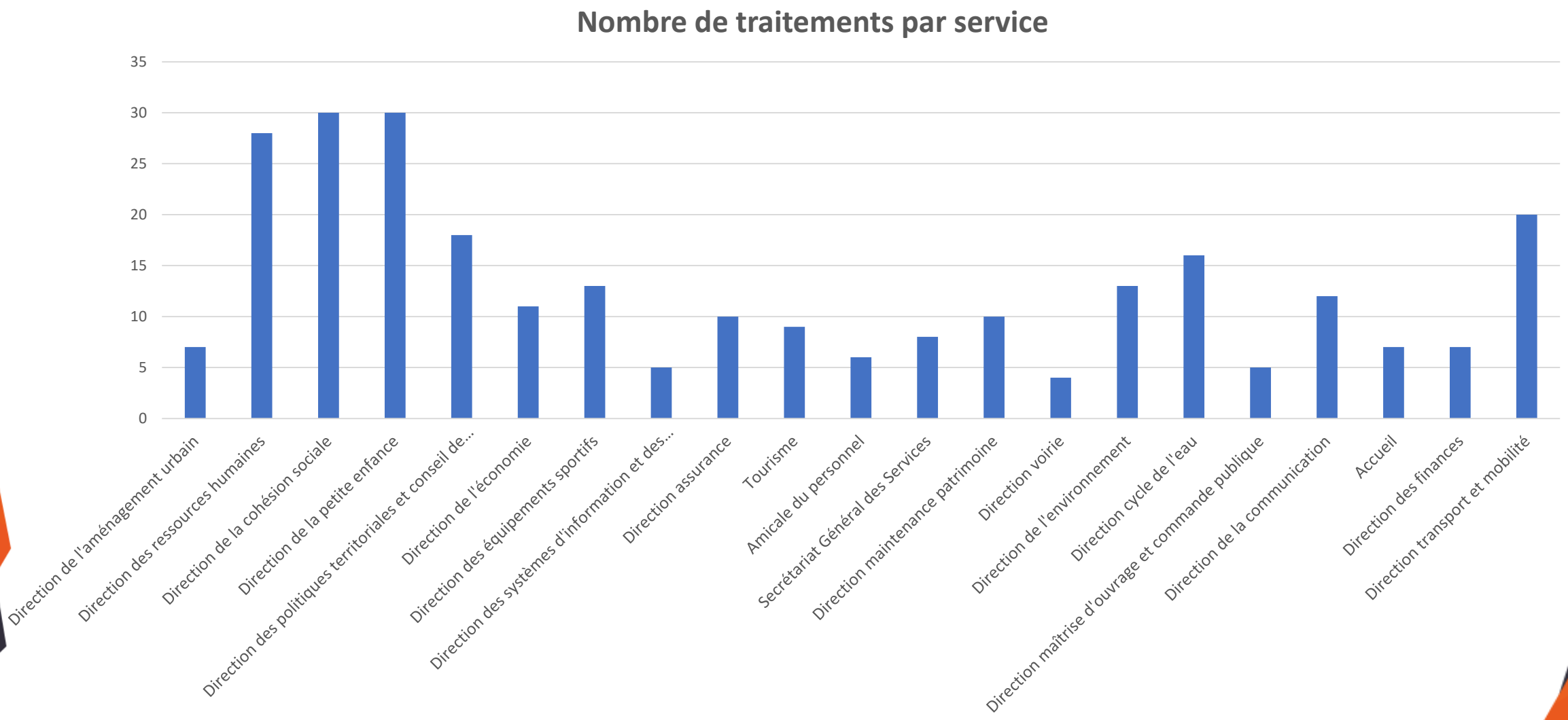
### 21 services audités

- Informatique
- Accueil
- Amicale du personnel
- Communication
- Politiques territoriales et conseil de développement
- Equipements sportifs
- DGST et Assurances
- Tourisme et DGA
- Voirie
- Maintenance patrimoine et vidéosurveillance
- Finances
- Maîtrise d'ouvrage et commande publique
- Economie
- Aménagement urbain
- DGS et secrétariat général
- Environnement
- Cycle de l’eau
- Cohésion sociale
- Petite enfance
- Ressources humaines
- Transport

# 2. Cartographie des traitements

# 2 Cartographie des traitements

Nombre de traitements identifiés par Direction



# 2 Cartographie des traitements

## Analyse des risques

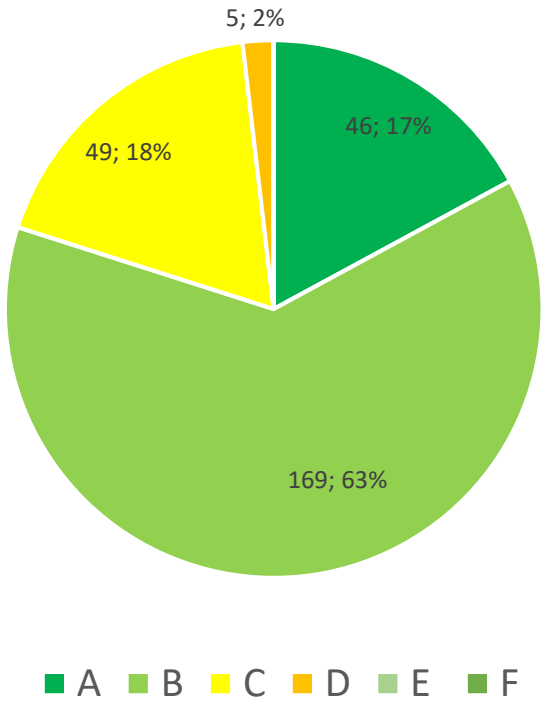
**3 types d'impacts sur les personnes**

- Préjudice Physique
- Préjudice Moral
- Préjudice Matériel

**3 types de menaces sur les données**

- Perte
- Altération
- Divulgation non autorisée

### Niveau de risque des traitements




**Notre méthodologie d'analyse des risques s'inspire des pratiques proposées par la CNIL et l'ANSSI (EBIOS)**

| | Description | Définition |
|---|---|---|
| A | Négligeable | Les personnes concernées ne sont pas ou très peu impactées. |
| B | Limité | Les personnes concernées subissent des désagréments facilement surmontables. |
| C | Sérieux | Les personnes concernées subissent des désagréments qu'elles pourront surmonter avec des difficultés. |
| D | Important | Les personnes concernées font face à des dommages significatifs qu'elles auront des difficultés à surmonter. |
| E | Sévère | Les personnes concernées font face à des dommages significatifs qu'elles auront beaucoup de difficultés à surmonter. |
| F | Maximal | Les personnes concernées font face à des dommages significatifs qu'elles pourraient ne pas surmonter. |

# 3. Analyse du niveau de maturité

# 3 Analyse du niveau de maturité

## 5 niveaux de maturité :

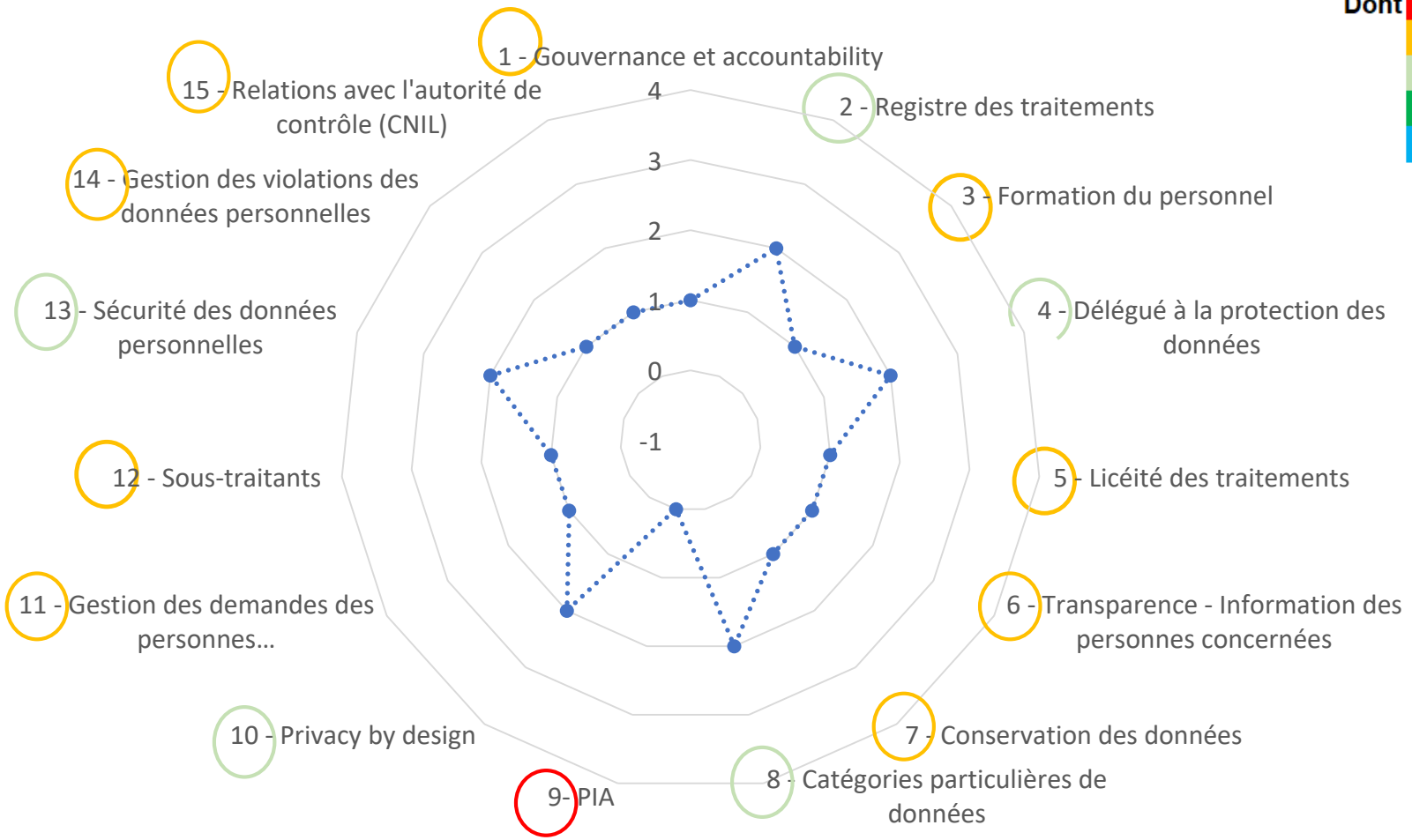
| | |
|---|---|
| **Inexistant** | L'organisme n'a pas connaissance des aspects réglementaires et ne les applique pas |
| **Emergent** | L'organisme a une connaissance même partielle des obligations réglementaires et les met en œuvre même de façon erronée |
| **Niveau Intermédiaire** | L'organisme maîtrise les principes de base de la protection des données et met en œuvre des processus conformes à la Loi Informatique et Libertés dans son ancienne version (2004) |
| **Niveau RGPD** | L'organisme est en conformité avec les Nouvelles exigences du Règlement européen sur la protection des données |
| **Avancé** | L'organisme va au-delà des exigences du Règlement européen |

## 15 Axes identifiés

1 - Gouvernance et accountability (responsabilité)
2 - Registre des traitements
3 - Formation du personnel
4 - Délégué à la protection des données
5 - Licéité des traitements
6 - Transparence - Information des personnes concernées
7 - Conservation des données
8 - Catégories particulières de données
9- PIA (analyse d'impact)
10 - Privacy by design (respect du RGPD dès la création)
11 - Gestion des demandes des personnes (Requêtes des personnes concernées dans l'exercice de leurs droits)
12 - Sous-traitants
13 - Sécurité des données personnelles
14 - Gestion des violations des données personnelles
15 - Relations avec l'autorité de contrôle (CNIL)

# 3 Analyse du niveau de maturité

## Ecart entre le niveau de conformité à Vienne Condrieu Agglomération et la réglementation en vigueur




| | | |
|---|---|---|
| Dont | 1 | stream(s) au niveau de maturité "Inexistant" |
| | 9 | stream(s) au niveau de maturité "Emergent" |
| | 5 | stream(s) au niveau de maturité "Intermédiaire" |
| | 0 | stream(s) au niveau de maturité "RGPD" |
| | 0 | stream(s) au niveau de maturité "Avancé" |

# 4. SWOT - Forces / Faiblesses / Opportunités / Menaces

# 4 SWOT – Forces / Faiblesses / Opportunités / Menaces

S

## Forces

- Réceptivité des agents rencontrés aux enjeux de la protection des données
- Nombre d'outils informatiques limité

W

## Faiblesses

- Tendance à la conservation des données
- Mentions d'information incomplètes ou inexistantes
- Pas ou peu de procédures/process mis en place de manière formelle

O

## Opportunités

- Revoir et uniformiser les processus internes en prenant en compte le RGPD
- Renforcer la confiance des usagers et des agents
- Revoir le cadre contractuel des sous-traitants

T

## Menaces

- Sécurité informatique :
  Pas de procédure de gestion des violations de données
- PIA à réaliser dans le cadre de la mise en place de caméras de vidéoprotection

# 5. Programme de mise en conformité

# 5 Programme de mise en conformité

Synthèse du plan d'action

21 services audités

De nombreux documents analysés (formulaires de collecte de données, contrats, etc.)

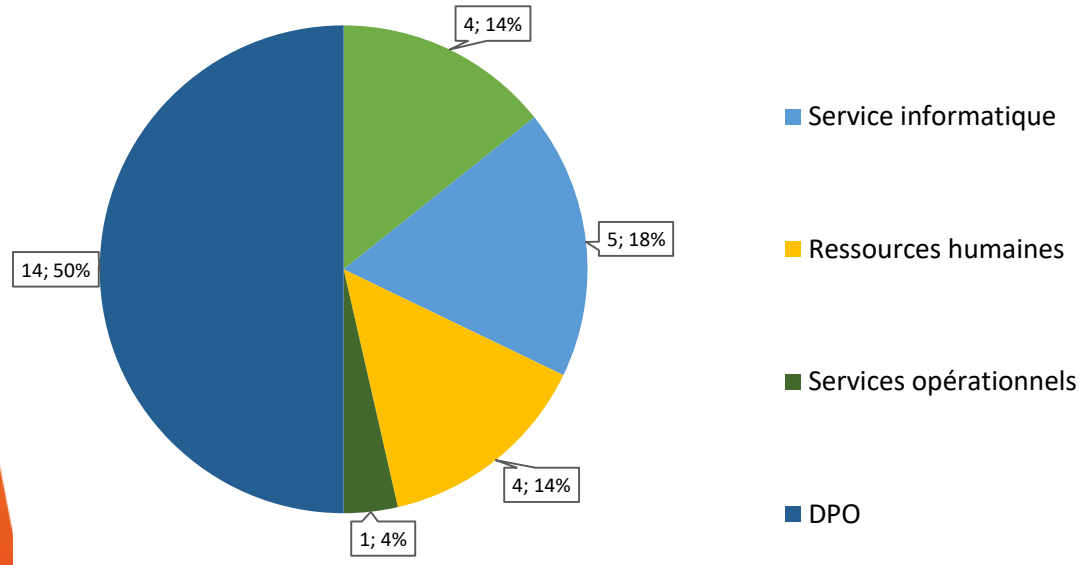
Une mise en conformité comprenant **28 actions**

Une durée estimée à au moins **9 mois à partir d'avril 2023**

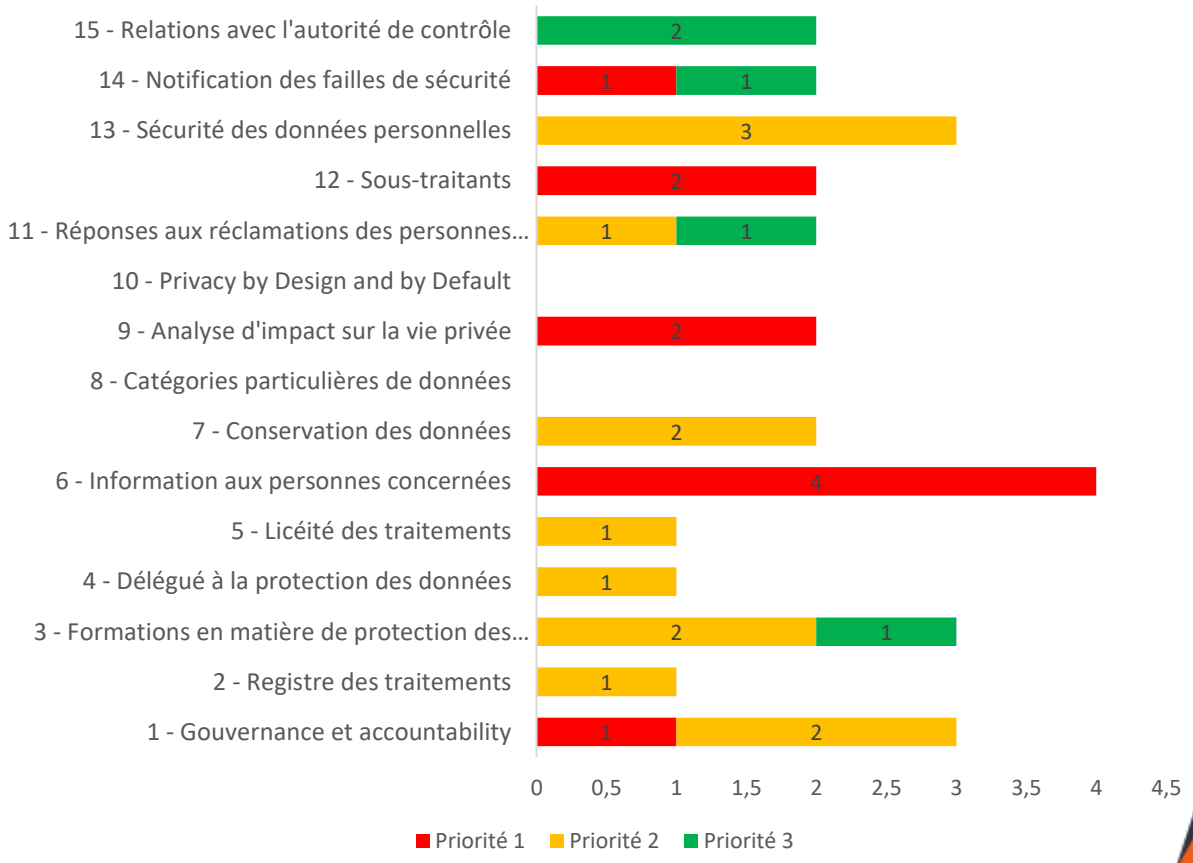
# 5 Programme de mise en conformité de Vienne Condrieu Agglomération

## Statistiques - Priorités

### Répartition des actions par Responsable




### Répartition des actions par axe et par priorité



5

# Programme de mise en conformité

## RACI : Réalisateur, Approbateur, Consulté, Informé

**R éalisateur** – La Personne qui réalise l'action.

**A pprobateur** – La Personne qui doit rendre des comptes sur l'avancement de l'action et qui est responsable de son accomplissement par le Réalisateur.

**C onsulté** – Les personnes qui sont consultées sur la manière de réaliser l'action.

**I nformé** – Les personnes qui sont informées.

# 6. Actions prioritaires

# 6 Actions prioritaires

| | |
|---|---|
| **Accountability (Responsabilité)** | •Valider et mettre en place un **plan d'actions** de la conformité |
| **Site internet** | •**Mettre à jour** la **politique de confidentialité** du site internet<br>•**Mettre à jour** la **politique cookies** sur le site internet |
| **•Transparence / Information** | •**Créer/mettre à jour** des **mentions d'information** (clause RGPD à destination des agents, des usagers etc.) |
| **Sous-traitant** | •Etablir une **grille d'évaluation** de la conformité des sous-traitants<br>•Conclusion/Mise à jour d'avenants RGPD nécessaires pour les contrats de sous-traitance |
| **AIPD (analyse d'impact relative à la protection des données)** | • •Etablir une **méthode pour la réalisation d'AIPD**<br>• •**Réaliser l'AIPD** relative à la mise en place de caméras de vidéoprotection |
| **•Sécurité des données** | •Rédiger une **procédure de gestion des violations de données** |

# 7. Prochaines étapes

# 7 Prochaines étapes

- **Valider le Plan d’actions**
  - les étapes et jalons clés
  - le RACI
  - les ressources budgétaires et humaines
  - la gouvernance en mode projet
- **Voter le budget nécessaire au déploiement du Plan d'actions**
- **Déployer le Plan d’actions**
  - Réalisation des chantiers
- **Phase 2 :**
  - Politique de confidentialité du site internet

***Merci pour votre attention***