# Document RGPD – Dictionnaire des Données Qualité de l’Air

## 1. Analyse RGPD – Conformité CNIL

### 1.1. Identification des données à caractère personnel

Après analyse du dictionnaire de données, aucune donnée personnelle directe ou indirecte (telle que nom, prénom, adresse IP, coordonnées, identifiant de personne physique) ne semble apparaître. Les données concernent :  
  
- La qualité de l’air (ex. aqi, pm25, pm10)  
- Des identifiants de stations (idx)  
- Des informations techniques ou agrégées (data, status)  
  
Conclusion : Pas de données personnelles identifiables dans l’état actuel.

### 1.2. Base légale du traitement

La collecte repose sur un intérêt légitime (analyse environnementale, suivi de la qualité de l’air) et potentiellement une mission d’intérêt public si le traitement est opéré par une autorité ou collectivité publique.

### 1.3. Minimisation des données

La structure actuelle montre une minimisation conforme (pas d’information superflue ni intrusive). Les données sont limitées à des indicateurs environnementaux.

### 1.4. Finalité du traitement

- Surveillance de la qualité de l’air  
- Fourniture d’indicateurs aux citoyens  
- Analyse pour des politiques environnementales  
  
Les finalités sont clairement définies et légitimes.

### 1.5. Conservation des données

À définir en fonction des besoins opérationnels. Recommandation : conserver les données agrégées autant que nécessaire, avec purge des données brutes si elles ne sont plus utiles.

### 1.6. Droits des personnes

Non applicable dans ce contexte car il n’y a pas de données personnelles.

## 2. Analyse de sécurité – Recommandations ANSSI

### 2.1. Authentification et accès

- Accès aux données via une API avec token → Vérifier que le token est bien sécurisé et renouvelé périodiquement.  
- Mettre en place une politique d’accès basée sur les rôles pour les utilisateurs internes.

### 2.2. Intégrité et traçabilité

- Journaliser les accès à l’API et les extractions de données.  
- Implémenter des hashs de contrôle sur les fichiers extraits pour garantir l'intégrité.

### 2.3. Hébergement et stockage

- S'assurer que les données sont stockées dans des infrastructures sécurisées (serveurs avec antivirus, pare-feu, mises à jour).  
- Privilégier l’hébergement en France ou UE.

### 2.4. Transmission sécurisée

- Utiliser HTTPS pour les appels API.  
- Éviter toute transmission en clair des tokens ou des résultats de l’API.

### 2.5. Supervision et audit

- Mettre en place une supervision des accès et des alertes en cas de comportement anormal.  
- Réaliser des audits réguliers de la sécurité du système.

## Synthèse

| Critère | Évaluation |
| --- | --- |
| Données personnelles | Non présentes |
| Finalités | Légitimes et environnementales |
| Sécurité (accès, stockage...) | Conforme sous réserve de contrôle |
| CNIL | Conforme au RGPD |
| ANSSI | Bonnes pratiques à mettre en place |

## 2. Analyse de sécurité – Conformité ANSSI (Modèle D/I/C/PAT)

### D – Disponibilité

- Assurer l’accès continu aux données via une infrastructure résiliente (serveurs redondants, sauvegardes).  
- Mettre en place un plan de continuité d’activité (PCA) pour maintenir les services pendant l’incident.  
- Disposer d’un plan de reprise d’activité (PRA) pour restaurer les opérations après un incident.

### I – Intégrité

- Vérifier l'intégrité des données par hachage (SHA-256, etc.).  
- Mettre en place des contrôles réguliers sur la cohérence des données issues de l’API.

### C – Confidentialité

- Chiffrement des transmissions via HTTPS.  
- Gestion sécurisée des tokens d’accès (expiration, stockage chiffré).

### P/A/T – Preuve / Auditabilité / Traçabilité

- Journalisation des accès et actions utilisateurs.  
- Mise en place d’audits réguliers.  
- Conservation des logs horodatés conformément aux règles internes.

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.