# **Synthèse RGPD – Projet SolarPerform**

## **1. Contexte légal**

SolarPerform est une plateforme numérique de collecte et de traitement de données énergétiques.  
 Elle collecte des **données personnelles** via :

* La création de comptes utilisateurs
* La configuration d’équipements IoT (via IP ou token)
* La réception de mesures liées à une installation physique (consommation, production…)

**Ces données peuvent identifier directement ou indirectement une personne** → SolarPerform est **responsable de traitement** au sens du RGPD.

## **2. Types de données personnelles collectées**

| **Catégorie** | **Données collectées** | **Finalité** |
| --- | --- | --- |
| Identité | Nom, prénom, email | Création de compte, communication |
| Authentification | Mot de passe (hashé), token JWT | Accès sécurisé |
| IoT & Connexion | Adresse IP de l'appareil, identifiants SFTP/MQTT | Liaison compte → équipement |
| Mesures d’activité | Consommation énergétique (kWh, timestamp), topic MQTT | Suivi, dashboard, alertes |
| Logs techniques | Dates de connexion, ID utilisateur, erreurs | Sécurité, support |

## 

## 

## **3. Fondements légaux RGPD**

| **Principe** | **Application dans SolarPerform** |
| --- | --- |
| **Licéité, loyauté, transparence** | Consentement explicite à l'inscription |
| **Minimisation des données** | Uniquement les données nécessaires sont collectées |
| **Limitation de finalité** | Aucune réutilisation hors du périmètre énergie / suivi utilisateur |
| **Sécurité** | Hash, chiffrement, contrôle d'accès |
| **Accès, portabilité, suppression** | Fonctionnalités GET /me, DELETE /me à exposer |
| **Durée de conservation** | Durée définie pour chaque type de donnée |

## **4. Mesures techniques à mettre en œuvre**

### **Sécurité des données**

* Mots de passe hashés (bcrypt)
* JWT avec expiration courte (ex : 15 min) + refresh
* Requêtes API protégées par Authorization: Bearer
* Chiffrement des tokens ou clés sensibles en base
* Logs d'accès anonymisés (optionnel : pseudonymisation)

### **Données en base PostgreSQL (schémas séparés)**

| **Schéma** | **Données sensibles ?** | **Chiffrement ?** | **Accès restreint ?** |
| --- | --- | --- | --- |
| auth | email, mot de passe | hashé | oui |
| user | IP, deviceId | possible | oui |
| mqtt | topic, identifiant | possible | oui |
| files, monitoring | Données liées au userId | pas critique, mais limiter l'accès | oui |

### 

### 

### 

### **Durée de conservation**

| **Donnée** | **Durée** |
| --- | --- |
| Logs de connexion | 6 mois |
| JWT & refresh tokens | 15 min / 7 jours |
| Données d’utilisateur inactif | Suppression après 3 ans sans activité |
| Données supprimées | Purge automatique sous 30 jours |

**5. Obligations documentaires**

**À inclure sur le site / app** :

* Politique de confidentialité claire
* Case à cocher "j’accepte la politique RGPD" lors de l'inscription
* Page Mon compte avec :
  + Voir mes données
  + Télécharger mes données
  + Supprimer mon compte

**À documenter en interne** :

* Registre de traitement RGPD (modèle à créer)
* Liste des services stockant des données personnelles
* Politique de conservation des données
* Modalité de notification en cas de fuite de données (DPIA possible à prévoir)

## **6. Rôles & responsabilités**

| **Rôle** | **Qui** | **Description** |
| --- | --- | --- |
| Responsable du traitement | L'entreprise mère (SolarPerform) | Décide des finalités du traitement |
| Sous-traitants | Hébergeurs, bases de données, GitHub... | Fournissent les outils ou services |
| DPO (optionnel) | À désigner si nécessaire | Garant du respect RGPD, point de contact CNIL |

## 

## **7. À implémenter dans le code/API**

* GET /me : retourne toutes les infos personnelles du user
* DELETE /me : supprime tout ce qui est lié à l’utilisateur
* GET /me/data-export : export JSON ou CSV (portabilité)
* middleware/verifyToken sur toutes les routes protégées
* emailVerified: false dans auth.users (si double opt-in prévu)

## **8. À produire**

| **Document** | **Format** |
| --- | --- |
| Politique de confidentialité | Markdown + lien dans le frontend |
| Registre de traitement RGPD | Excel / Notion / GDocs |
| Documentation API RGPD | Swagger + doc développeur |
| DPIA (si besoin) | PDF CNIL – à remplir si données sensibles / en masse |