POLITIQUE DE PROTECTION DES DONNÉES DU SIEIL

Octobre 2022

Le 10 octobre 2022

Signé électroniquement

Par délégation du Président,
La Directrice Générale des Services

Sophie NICOLAS

Sommaire

Glossaire

RGPD	Règlement Général sur la Protection des Données
CEPD	Comité Européen à la Protection des Données
CNIL	Commission Nationale de l'Informatique et des Libertés
DPD	Déléguée à la Protection des Données
SIEIL	Syndicat Intercommunal d'Énergie d'Indre-et-Loire

Introduction

Objectifs de la politique

La présente politique a pour objectif de définir les principes généraux de protection des données personnelles et de gestion des traitements de données personnelles du SIEIL :

- Dans sa mise en conformité, à travers le pilotage du projet de mise en conformité du SIEIL au RGPD, l'identification de l'ensemble des procédures et des outils, des acteurs et des instances de gouvernance ;

- Dans son maintien en conformité.
  - Encadrement des nouveaux projets par la structuration du processus de *Privacy by design* : cadrage de tout nouveau traitement avec notamment vérification de sa licéité, définition des finalités, gestion des durées de conservation, des mesures de sécurité et des sous-traitants, information des personnes, et éventuellement mise en œuvre d'une analyse d'impact.
  - Protection des données au quotidien : maintien des registres, sensibilisation des agents, gestion des droits des personnes, gestion des violations de données, coopération avec la CNIL, contrôle interne.

Au-delà de sa visée documentaire, la politique de protection des données du SIEIL est donc un outil de cadrage pour les différentes procédures mises en œuvre en interne.

Destinataires de la politique

La présente politique s'adresse à l'ensemble des collaborateurs du SIEIL, à savoir notamment :

- Les instances de gouvernance du SIEIL,
- Les agents du SIEIL,
- L'ensemble des prestataires et partenaires du SIEIL susceptibles de traiter des données personnelles pour son compte.

La politique s'adresse également, dans une visée informative, à l'ensemble des collectivités adhérentes et à leurs élus.

La politique de protection des données du SIEIL est communiquée à ces destinataires sur demande et est accessible pour l'ensemble des collaborateurs internes sur le WikiSIEIL.

Périmètre de la politique

La présente politique porte sur deux catégories de traitements de données personnelles :

- Ceux mis en place par le SIEIL au titre de son fonctionnement interne, et qui concernent essentiellement les données personnelles des agents, élus, délégués… ;
- Ceux mis en place par le SIEIL au titre de ses compétences et missions, et qui concernent principalement les données personnelles des tiers (usagers, communes, entreprises...).

L'ensemble des règles à respecter s'appliqueront par principe à ces deux catégories de traitements, pour lesquels le SIEIL est « Responsable de traitement » au sens du RGPD.

Rappel des notions

La Politique de protection des données du SIEIL utilise plusieurs notions issues de la réglementation sur la protection des données. Ces notions ont le sens que leur donne la CNIL dans le glossaire accessible sur son site web, notamment :

- Donnée personnelle : toute information se rapportant à une personne physique identifiée ou identifiable.
- Traitement de données : opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé.
- Responsable de traitement : personne morale ou physique qui détermine les finalités et les moyens d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser.

Présentation générale

Cadre réglementaire

Le Parlement Européen a adopté le 27 avril 2016 un règlement relatif à la protection des personnes physiques à l'égard du traitement de leurs données personnelles et à la libre circulation de ces données, généralement nommé « Règlement Général sur la Protection des Données » (**RGPD**).

A la suite du RGPD, l'Assemblée Nationale a adopté la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, modifiant ainsi la loi n°78-17 du 6 janvier 1978 dite « Loi informatique et Libertés ».

En France, la Commission Nationale de l'Informatique et des Libertés (**CNIL**) est l'autorité publique en charge d'assurer la régulation autour des données personnelles en France. Ses lignes directrices et recommandations, qui viennent préciser les obligations du RGPD, font partie intégrante du cadre applicable.

Au niveau européen, le Comité Européen à la Protection des Données (**CEPD**) veille à l'application uniforme et cohérente du RGPD, notamment par la publication de lignes directrices.

Cette réglementation est complétée par les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**) sur les questions liées à la sécurité numérique.

Le Syndicat Intercommunal d'Energie d'Indre-et-Loire (**SIEIL**), en tant qu'organisme public, réalise des missions nécessitant le traitement de données personnelles et doit donc respecter les exigences imposées par cette réglementation.

Ambition du SIEIL relative à la protection des données personnelles

Le SIEIL a pour double ambition d'assurer une protection forte de la vie privée et des libertés fondamentales des personnes dont elle traite les données et de maintenir parfaitement sa conformité à la réglementation et aux bonnes pratiques publiées par la CNIL.

Pour porter ces ambitions, le SIEIL adopte les engagements suivants :

- Déployer une organisation adaptée s'appuyant sur des processus structurés,
- Impliquer et responsabiliser l'ensemble de ses agents et de ses partenaires,
- Maintenir une démarche d'amélioration continue de ces processus.

Lancement du projet au SIEIL

Le SIEIL a engagé, dès mai 2018, une démarche de mise en conformité au RGPD, conscient de la nécessité de protéger davantage les données personnelles de ses agents et des usagers. Cette prise en compte de la protection des données a notamment été initiée par :

- La désignation d'une Déléguée à la Protection des Données (DPD) auprès de la CNIL et la constitution d'un groupe de travail RGPD,
- L'audit du niveau de conformité du SIEIL par la société ACTECIL.

Grâce à une bonne implication de la DPD, des services et de la direction du SIEIL, de nombreuses actions ont été réalisées depuis 2018 et le rythme de mise en conformité et de maintien en conformité reste soutenu.

Corpus documentaire lié à la protection des données

La Politique de protection des données du SIEIL définit un ensemble de principes à respecter pour assurer la protection des données personnelles.

Plusieurs points de la présente politique sont déclinés en procédures ou politiques distinctes :

- Procédure d'intégration du RGPD dans les nouveaux projets,
- Procédure de gestion des violations de données,
- Procédure de gestion des demandes d'exercice de droits,
- Procédure de gestion des durées de conservation,
- Procédure de gestion des zones bloc note et commentaires,
- Procédure de publication de données sur le web,

Les procédures s'accompagnent d'outils permettant de les mettre en œuvre :

- Registre des traitements de données,
- Registre des demandes de droits des personnes,
- Registre des violations de données,
- Outils d'audits et d'analyse d'impact,
- Tableau de suivi de la conformité des traitements,
- Tableau de suivi de la sensibilisation,
- Feuille de route de la conformité du SIEIL,
- Questionnaire à destination des sous-traitants.

Une charte informatique a également été mise en place, avec pour objectif de diffuser les bonnes pratiques informatiques auprès des agents en termes d'usages, de sécurité et de protection des données personnelles. Elle est complétée par un guide à destination des agents « la gestion des données à caractère personnel au SIEIL ».

Gouvernance de la protection des données

Organisation, rôles et responsabilités liés au RGPD

Le SIEIL, dans le cadre de ses missions mais aussi de son fonctionnement interne, met en œuvre des traitements de données personnelles : il en définit les objectifs (finalités) et les moyens essentiels. A ce titre, le SIEIL est donc qualifié de **Responsable de traitement** au sens du RGPD : il doit donc s'assurer de la conformité des traitements qu'il met en œuvre et mettre en place une organisation interne permettant de répondre aux exigences du RGPD.

Le projet de mise en conformité et de maintien en conformité est piloté par la **Déléguée à la Protection des Données** (**DPD**) du SIEIL, Aude POUCE, désignée par le Comité syndical en juin 2018 et auprès de la CNIL dès juillet 2018. La DPD a été formée à cet effet, dispose de ressources propres et est accompagnée par une entreprise externe dans ses missions de déléguée à la protection des données. Conformément au RGPD, la DPD est rattachée au plus haut niveau de la direction.

En interne, la DPD est appuyée par un **Groupe de travail RGPD**, composé :

- De la Direction Générale des Services,
- Du service Finances,
- Du service des ressources humaines,
- Du service informatique,
- Du secrétariat de direction,
- Du service transition énergétique.

Ce groupe de travail a permis une avancée satisfaisante du projet de mise en conformité depuis 2018 ainsi qu'une bonne diffusion des principes au sein des différents services.

Maintien de la documentation

Une revue annuelle de la présente politique et des procédures internes est effectuée.

Une revue pourra également être effectuée en cas :

- D'évolution législative ou réglementaire significative impactant la protection des données, ou de publication de la CNIL ou du CEPD précisant ce cadre réglementaire,
- D'évolution organisationnelle majeure au sein du SIEIL.

Politique de sensibilisation des agents

De nombreux agents du SIEIL sont amenés, dans l'exercice de leurs missions, à manipuler ou accéder à des données personnelles. En fonction de leurs responsabilités dans la mise en œuvre des traitements de données, ces agents doivent être sensibilisés ou formés à la protection des données.

En conséquence, le SIEIL a mis en place en interne une politique ambitieuse de sensibilisation à la protection des données.

Cette politique repose sur trois principes :

- Sensibilisation de 100% des agents à leur arrivée,
- Sensibilisation régulière des agents,
- Formation continue de la DPD.

Principe n°1 : Sensibilisation de 100% des agents à leur arrivée

Dans la procédure d'entrée d'un nouvel agent au sein du SIEIL a été intégrée un volet RGPD, impliquant la remise de la documentation qui s'y rapporte (charte informatique, guide de la gestion des données à caractère personnel), mais également la sensibilisation de l'agent, dans les mois suivant son intégration. Cette sensibilisation à la protection des données est réalisée par la DPD, sous un format ludique favorisant l'implication de l'agent.

Principe n°2 : Sensibilisation régulière des agents

Au-delà de cette sensibilisation initiale, le SIEIL s'assure que ses agents gardent un haut niveau de sensibilisation à la protection des données, à travers un plan de sensibilisation impliquant :

- Un renouvellement de la session de sensibilisation lorsque cela apparait nécessaire,
- La mise en œuvre d'actions régulières, sur le thème des données personnelles et de la sécurité numérique.

Principe n°3 : Formation continue de la DPD

En phase avec les recommandations de la CNIL et du CEPD, la DPD du SIEIL est spécialement formée à la protection des données, et se forme en continu, ce qui lui permet de maintenir ses connaissances à jour en ce qui concerne les évolutions réglementaires et techniques.

Cette formation est effectuée notamment à travers le suivi de MOOC et de webinaires.

Cadrage des traitements de données

Les principes définis dans la présente section ont pour objectif d'assurer un cadrage de tout projet de mise en place d'un traitement de données personnelles.

Prise en compte du RGPD dans chaque projet

Le SIEIL met en œuvre une procédure d'intégration du RGPD dans les nouveaux projets, qui vise à assurer que l'ensemble des principes applicables aux traitements de données soient pris en compte dès la conception du traitement de données (principe de *Privacy by design*).

Concrètement, lorsqu'un projet implique l'utilisation de données personnelles, la DPD doit en être informée le plus tôt possible dans la phase de conception. Cela permet que chaque utilisation et support de données personnelles soient audités et adaptés afin que le projet soit conforme au RGPD dès son lancement.

Ce principe s'applique aux nouveaux projets, mais également aux modifications substantielles de projets existants.

Principes applicables aux traitements de données

Chaque traitement de données personnelles doit respecter les règles issues du RGPD et de la réglementation applicable, notamment :

Finalité. Les données personnelles doivent être collectées et utilisées dans un objectif précis (la finalité). La finalité doit être déterminée, explicite et légitime.

Base légale. Le traitement doit reposer sur l'une des six bases légales prévues par le RGPD (obligation légale, mission d'intérêt public, contrat, sauvegarde des intérêts vitaux, intérêt légitime, consentement).

Minimisation. Seules les données nécessaires et pertinentes vis-à-vis de la finalité définie doivent être collectées : c'est le principe de minimisation de la collecte.

Données sensibles. Les données sensibles en particulier, ne doivent être collectées que dans des cas strictement limités, et doivent faire l'objet d'une protection particulière.

Durées de conservation. Si les données ne font pas l'objet d'un archivage public, elles doivent nécessairement avoir une durée de vie limitée, définie dès la phase projet.

Sous-traitance. Si le SIEIL fait appel à un sous-traitant (au sens du RGPD) pour réaliser des opérations de traitement, il s'assure que la relation soit convenablement encadrée et que ce sous-traitant présente des garanties suffisantes en termes de sécurité et de conformité.

Information. Les personnes doivent être informées, dès la collecte, des finalités et des moyens du traitement de données.

Droits des personnes. Chaque personne concernée par le traitement dispose de droits sur ses données, qui doivent être garantis par le SIEIL. Certains de ces droits s'appliquent systématiquement (droit d'accès, droit de rectification), les autres s'appliquant dans certaines circonstances (droit d'opposition, droit à l'effacement, droit à la limitation du traitement, droit à la portabilité des données).

Sécurité et confidentialité. Tout traitement de données doit être encadré par des mesures de sécurité techniques et organisationnelles, adaptées au risque du traitement. Ces mesures doivent garantir la confidentialité, la disponibilité et l'intégrité des données personnelles.

Analyses d'impact sur la protection des données

Une analyse d'impact doit être réalisée pour les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Elle se décompose en trois partie :

- Une description détaillée du traitement,

- Une évaluation juridique de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux,
- Une étude technique des risques sur la sécurité des données.

Pour déterminer l'opportunité de réaliser une analyse d'impact, le SIEIL s'appuie sur :

- la liste de traitements pour lesquels la CNIL a estimé obligatoire de réaliser une analyse d'impact,
- les critères issus des lignes directrices du CEPD,
- une analyse au cas par cas des risques du traitement, réalisée par la DPD.

Principe de contrôle de la bonne application des mesures

Conformément à la réglementation, la DPD est investie d'une mission de contrôle du respect du RGPD. La DPD peut donc vérifier à tout moment :

- L'exactitude de la documentation tenue par le SIEIL,
- La conformité des traitements mis en œuvre par le SIEIL,
- L'effectivité des mesures techniques et organisationnelles que le SIEIL s'est engagé à mettre en œuvre.

A ce titre, la DPD peut collaborer avec d'autres fonctions clés du SIEIL, notamment pour les questions de sécurité informatique.

Protection des données au quotidien

Registres du SIEIL

Le SIEIL s'assure de documenter toute évolution ou tout nouveau traitement dans le registre des traitements.

En ce qui concerne les traitements pour lesquels le SIEIL fait appel à des sous-traitants, une liste des sous-traitants est maintenue à jour, précisant notamment les mesures permettant de s'assurer d'un niveau de protection adéquat.

Tableau de bord et feuille de route

Afin de suivre de manière concrète l'avancée de la conformité du SIEIL au RGPD, des outils de suivi sont mis en place par la DPD :

- Des tableaux de suivi thématiques (conformité des traitements, sensibilisation). Ces tableaux de suivi permettent de générer des indicateurs clés sur la conformité au RGPD, thématique par thématique : nombre de traitements identifiés, audités et conformes, taux d'agents sensibilisés, etc.

- Une feuille de route a également été établie pour suivre de manière transversale l'avancée de la conformité du SIEIL au RGPD, identifier les actions à mener et les prioriser.

Tableaux de suivi et feuille de route permettent également de documenter la conformité du SIEIL au titre du principe de responsabilité (« *Accountability* »).

Gestion des demandes d'exercice de droits

Le SIEIL s'assure de traiter les demandes de droits exercées par les personnes concernées, dans les délais réglementaires.

Une procédure spécifique de gestion de ces droits est mise en œuvre en interne.

Gestion des violations de données personnelles

Le SIEIL s'assure que toute violation de données fait l'objet :

- D'une mention dans le registre des violations de données,
- D'une notification auprès de la CNIL (s'il existe un risque pour les personnes),
- D'une communication aux personnes concernées (si le risque est important).

Une procédure spécifique de gestion des violations de données est mise en œuvre en interne.

Contacts avec la CNIL

Pour toute sollicitation effectuée par la CNIL, la DPD du SIEIL est le point de contact prioritaire et à privilégier. Toute demande émise par la CNIL au SIEIL est ainsi remise sans délai à la DPD qui se chargera d'en informer par ailleurs le métier concerné, le cas échéant.

En cas de violation de données ou de contrôle, la DPD coopère avec la CNIL et lui fournit toute documentation nécessaire.

Contacts avec les tiers

Pour toute demande de renseignements complémentaires, sur le contenu de la politique ou plus largement sur la protection des données au sein du SIEIL, n'hésitez pas à contacter la DPD.

Aude POUCE
rgpd@sieil37.fr
SIEIL, Déléguée à la Protection des Données, 12 rue Blaise Pascal, 37000 Tours.