POLITIQUE GROUPE DE PROTECTION DES DONNÉES A CARACTERE PERSONNEL
Version publique
Juillet 2022

1. Introduction

1.1. Le contexte, les enjeux et les défis

Le Groupe attache la plus grande importance à la protection des données personnelles et de la vie privée, valeurs définies dans sa Charte Ethique.

Le Groupe ENGIE traite les Données à caractère personnel relatives à ses collaborateurs, clients, partenaires, prestataires de services et fournisseurs dans le cadre de ses activités quotidiennes (gestion des candidats, du personnel, gestion des solutions prospects et clients, etc.).

Les Personnes Concernées sont de plus en plus conscientes des Données qu'elles partagent et s'attendent à un Traitement et à une protection appropriés de leurs données personnelles.

Les pouvoirs publics sont de plus en plus vigilants à propos de ces questions. Ils imposent des obligations plus strictes aux entreprises qui traitent des données personnelles et peuvent les poursuivre par le biais de sanctions civiles, pénales et financières. Ainsi, le Groupe et ses Entités doivent se conformer à ces réglementations[1].

Par conséquent, le Groupe se trouve de plus en plus exposé aux risques internes/externes liés à la collecte inappropriée, au stockage, à l'utilisation, à la modification, à la compromission et même à la falsification de Données à caractère personnel.

Fort de ses valeurs relatives aux Données à caractère personnel et à la vie privée et conscient de l'importance des règles de protection de celles-ci et des risques encourus en cas de violation, le Groupe s'est engagé à les protéger et à ce titre met en œuvre la présente politique (la « Politique »).

1.2. Champ d'application et objectifs

Les principes de la Politique sont fondés sur les conventions internationales. En cas de conflit entre la Politique et les conventions internationales, ou réglementations nationales applicables à une Entité, celles-ci prévalent sur ces principes .

Sous réserve de toute modification régionale, la Politique Groupe de protection des données à caractère personnel s'applique à l'ensemble de son personnel et de ses Entités.

Cette Politique sera progressivement accompagnée et détaillée par des documents complémentaires (framework du programme privacy, méthodologies, procédures, bonnes pratiques, sensibilisation, etc. développés au niveau du Groupe, du Hub Régional, de la Business Entity, de GBS ou de l'Entité) devant permettre l'atteinte des objectifs fixés.

Les exigences suivantes doivent être respectées avant la mise en œuvre effective de tout Traitement et doivent donc être prises en compte dans la planification de tout projet impliquant le Traitement de Données à caractère personnel. Une fois mis en œuvre, le Traitement doit à tout moment respecter les principes décrits dans la Politique. Des exigences similaires peuvent également s'appliquer en cas de modification des conditions dans lesquelles le Traitement est effectué.

[1] Lois sur la protection des données personnelles (Règlement Européen et autres nationales sur la Protection des données personnelles).

2. Gouvernance

Les objectifs et moyens de protection des Données à caractère personnels décrits ci-dessous sont à mettre en œuvre à tous les niveaux du Groupe.

2.1. Au niveau du Groupe

La gestion stratégique de la Politique relève de la responsabilité du Comité Exécutif d'ENGIE qui délègue la coordination et la gestion opérationnelle de la Politique au DGA en charge du Secrétariat Général du Groupe et au DGA en charge des Systèmes d'Information et du Digital du Groupe, qui à leur tour délèguent cette mission au Data Privacy Manager Groupe.

2.1.1. Data Privacy Manager Groupe

Les principales taches du Data Privacy Manager Groupe sont d'assurer la mise en œuvre de la présente Politique et de coordonner les activités connexes avec les GBU, les Hubs Régionaux, les Business Entities et GBS.

2.1.2. Le Comité Privacy Sponsor

La présente Politique établit un Comité Privacy Sponsor chargé d'assurer la coordination et la gouvernance opérationnelle de la Politique Groupe de protection des données à caractère personnel.
Ce Comité est composé de deux sponsors de la protection des données personnelles : le DGA en charge du Secrétariat Général du Groupe et le DGA en charge des Systèmes d'Information et du Digital du Groupe.
Il doit régler / décider de certaines situations complexes et peut communiquer à la filière sur les points d'attention de la protection des Données à caractère personnel.

2.1.3. Le Comité de Protection des Données

La présente Politique établit un Comité de Protection des Données ayant pour objectif d'assurer le pilotage des activités transverses liées à la protection des Données. Présidé par le Data Privacy Manager Groupe, le Comité de Protection des Données réuni les Data Privacy Managers de l'organisation et les représentants des Directions du Corporate (RH, SI & Digital, Ethique …). Le Comité de Protection des Données décide des actions transverses à son niveau et en réfère aux instances Groupe.

2.1.4. Le Comité Opérationnel de la protection des données (PROCOM)

La présente Politique établit un comité opérationnel décidé à valider la conformité des Traitements de données personnelles intragroupe. Présidé par le Data Privacy Manager Groupe, le PROCOM réunit les Data Privacy Managers de l'organisation et les représentants des Directions du Corporate (RH, IS & Digital, …) en fonction des Traitements de données intragroupe à examiner.

2.2. Aux autres niveaux d'Engie

Chaque Entité de l'organisation est responsable, à son niveau, de son activité en matière de protection des données à caractère personnel et doit s'assurer du respect de la Politique Groupe de protection des données.

Tous les membres du personnel (temporaires et permanents) sont responsables, à leur niveau, des Données à caractère personnel auxquelles ils accèdent et qu'ils traitent.

Tout membre du personnel mettant en œuvre une application qui traite des Données à caractère personnel doit d'abord se référer à son DPM / DPO car le Traitement peut nécessiter une notification préalable auprès d'une Autorité de Contrôle.

2.3. Autres parties prenantes

Les Cyber and Information Security Officers (CISO) doivent proposer leur expertise et leur aide dans le domaine de la Protection des données à caractère personnel, que les Traitements soient hébergés en interne ou auprès d'un tiers.
Les chefs de projet agissent pour le compte du Responsable de Traitement et géreront les projets impliquant le Traitement de données à caractère personnel. Ils doivent s'assurer que la Protection des Données est maintenue tout au long du projet et disposer des ressources et du temps nécessaires pour prendre en compte les exigences en la matière.

Les Responsables Achat doivent intégrer dans leur process d'appel d'offre les attentes en matière de cybersécurité et de protection des données personnelles liées au projet. Ils veillent à ce que les contrats comprennent – avant la signature – les éléments nécessaires à la conformité.

Tout tiers, y compris les Sous-traitants, réalisant des services au nom d'une Entité doit être informé des principes de la présente Politique en ce qui concerne les Données à caractère personnel qu'il accède et traite.

3. Programmes privacy et Accountability

Les Data Privacy Managers définissent, mettent en œuvre et suivent les programmes de conformité privacy, afin d'en garantir une gestion efficace et en constante amélioration.

L'Accountability est le principe fondateur en particulier dans la règlementation européenne. Les Entités (en tant que Responsables de Traitement ou Sous-traitants) doivent mettre en œuvre toutes les mesures appropriées et efficaces, être en mesure de démontrer la conformité du Traitement des Données et l'efficacité des mesures prises.

La mise en œuvre de la présente Politique est l'une des composantes essentielles de l'engagement du Groupe en matière de protection des Données, et de la mise en conformité avec le Règlement européen et les autres législations nationales.

4. Moyens et principes de protection des données

1. Sensibilisation et formation

L'ensemble du personnel doit être sensibilisé aux questions relatives à la protection des Données.

2. Contrôles, risques et audits

En ce qui concerne le contrôle interne, un référentiel de protection des données est géré par le DPM du Groupe. Il s'agit d'un ensemble de contrôles clés à mettre en œuvre sur un périmètre Groupe défini par le DPM du Groupe selon une approche basée sur les risques. Les DPM / DPO de l'organisation sont responsables d'effectuer une auto-évaluation annuelle afin de confirmer l'efficacité de ces contrôles clés et de définir des actions d'amélioration si nécessaire.

L'exercice annuel ERM (Enterprise Risk Management) est préparé par le DPM du Groupe en coordination avec la Direction de Gestion des Risques. Il est de la responsabilité des DPM / DPO de l'organisation de conduire l'exercice et de mettre en œuvre les plans d'action nécessaires.

La conduite effective de ces actions peut faire l'objet d'audits menés par la Direction de l'Audit Interne.

3. Cartographie de Traitement

Il est recommandé que chaque Entité de l'organisation établisse une cartographie et un registre[2] de tous les Traitements de données importants afin d'offrir une vue d'ensemble complète et de permettre de contrôler et de rationaliser les Traitements de données, ainsi que de faciliter la gestion des demandes d'accès de la Personne Concernée par le Responsable de Traitement.

4. Gestion des incidents

Toute personne ayant connaissance d'une utilisation inappropriée de Données à caractère personnel doit contacter son DPM / DPO qui signalera cet incident à son Ethics Officer. Les Data Privacy Managers sont informés des violations de Données et agissent en conséquence en coopération avec les Chief Information Security Officers.

Les DPM / DPO des Entités devront notifier, le cas échéant, les violations de Données à leur Autorité de Contrôle dans le délai indiqué par leur législation nationale et, si nécessaire, notifier également les Personnes Concernées.

5. Accords écrits

Des accords écrits doivent être établis entre les parties concernées par la mise en œuvre d'un Traitement de données (ENGIE, ses clients ou partenaires). En toutes circonstances, la collecte, l'utilisation ou la sous-traitance des Données personnelles doivent être conformes aux lois en vigueur, à la Charte Ethique d'ENGIE et à la présente Politique.

[2] Pour certaines Entités, le registre est une obligation, selon la législation locale, telle que la réglementation européenne

D’autres principes de protection des données doivent être mis en oeuvre au sein d’ENGIE (sauf si les lois nationales sont contraires ou plus strictes) :

1. Finalités explicites, légitimes, loyales et transparentes
2. Pertinence, minimisation et proportionnalité des données collectées
3. Conservation limitée des données
4. Données sensibles, fichiers sensibles et traitements à risque
5. Obligation de sécurité et de confidentialité
6. Classification et protection des données personnelles
7. Traitement du risque en amont (Privacy by Design, by Default, Analyse d’Impact relative à la Protection des Données)
8. Transferts internationaux
9. Transparence et respect des droits des personnes (Notice d’information, consentement, droit d’accès, …)
10. Obligations des Sous-Traitants