GROUP DATA PRIVACY POLICY
Public release
July 2022

1. Introduction

1.1. The context, issues and challenges

The Group is deeply committed to protecting Personal Data and personal privacy, which are values set out in its Ethics Charter.

The ENGIE Group processes Personal Data relating to its employees, customers, partners, service providers and suppliers in the course of its daily activities (candidate, personnel management, prospect and customer solutions management, etc.).

Individuals are more and more aware of the data they share, and expect proper processing and protection of their Personal Data.

Public authorities are increasingly aware of these matters. They are imposing more stringent obligations on companies that process Personal Data and may pursue them by way of civil, penal and financial sanctions. Thus, the Group and its Entities must comply with these regulations[1].

Consequently, the Group finds itself increasingly exposed to the risks associated with the inappropriate internal or external collection, storage, usage, modification, compromising and even falsification of Personal Data.

Based on its ethical values regarding personal data and privacy, and keenly aware of the importance of the rules on protecting data and privacy and the risks run in the event of data breaches, the Group pledges to protect such data and privacy, and accordingly is deploying this policy (the "Policy").

1.2. Scope and objectives

The principles of the present Policy are based on the international conventions. In the event of any conflict between the Policy and the applicable international conventions or national regulations applicable to an Entity, the latter will take precedence over these principles.

Subject to any regional modifications, the Group Data Privacy Policy applies to all its personnel and Entities.

This Policy will be reinforced and made more detailed with additional further documents (privacy program framework, methodologies, procedures, good practices, awareness, etc. developed either at the Group, the Regional Hub, the Business Entity, GBS or the Entity levels) that will enable the achievement of the objectives set.

The following requirements shall be complied with prior to the effective implementation of any intended Data Processing and shall thus be taken into account in the planning of any project involving processing Personal Data. Once implemented, the Data Processing should at all times respect the principals outlined below in this Policy. Similar requirements may also apply in the event of a change of the conditions under which the Data Processing is performed.

[1] Data Privacy Laws (European Regulation and other national data privacy laws).

2. Governance

The objectives and means of protecting Personal Data described below are to be implemented at all levels of the Group.

2.1. At Group level

The strategic management of the Group Data Privacy Policy is the responsibility of the ENGIE Executive Committee which delegates the coordination and operational management of the Policy to the Executive Vice President Group Corporate Secretary and the Executive Vice President IT and Digital, who in turn delegate this task to the Group Data Privacy Manager.

2.1.1. Group Data Privacy Manager

The main duties of the Group Data Privacy Manager are to ensure the effective implementation of the present Policy and coordinate the related privacy activities with the GBUs, the Regional Hubs, the Business Entities and GBS

2.1.2. The Privacy Sponsor Committee

The present Policy establishes a Privacy Sponsor Committee to provide coordination and operational governance of the Group Data Privacy Policy. This Committee is composed of two privacy sponsors : the Executive Vice President Group Corporate Secretary and the Executive Vice President IT and Digital. It has to settle/decide on some complex situations and may communicate on global privacy attention points to the privacy line.

2.1.3. The Privacy Committee

The present Policy establishes a Privacy Committee to manage transversal activities concerned with Data Protection. Chaired by the Group Data Privacy Manager, the Privacy Committee will convene the Data Privacy Managers of the organization and representatives of Corporate Divisions (HR, IS & Digital, Ethics, …). The Privacy Committee decides of transversal actions at its level and submits them to Group-level bodies.

2.1.4. The Privacy Operational Committee (PROCOM)

The present Policy establishes an operational committee dedicated to validate the compliance of cross-group data processing. This Committee is chaired by the Group Data Privacy Manager who convenes the Data Privacy Managers of the organization and representatives of Corporate Divisions (HR, IS & Digital, ..) accordingly with the cross-group data processing to review..

2.2. At other levels of ENGIE

All entities of the organization are responsible, on their respective scopes, for their data privacy activities and shall ensure compliance with the Group Data Privacy Policy.

All personnel (both temporary and permanent) are responsible, at their level, for Personal Data they access and process.

All personnel implementing an application that processes Personal Data must first refer to their DPM / DPO as Data Processing may require prior notification to a Data Protection Authority.

2.3. Other stakeholders

The Cyber and Information Security Officers (CISOs) shall offer their expertise and support in the area of Data Privacy, both for the purposes of data processing hosted internally and with a third party.

The Project Managers act on behalf of the Data Controller and will manage projects which entail the processing of Personal Data. They must ensure that Data Privacy is maintained throughout the project and have necessary resources and time to take into account privacy requirements.

The Procurement Officers shall include in their Request for Proposal (RFP) process the cybersecurity and data protection expectations related to the project. They shall ensure that contracts include – before signature - the necessary privacy compliance components.

Any third party, including Data Processors, providing services on behalf of an Entity has to be made aware of the principles of this Policy with respect to Personal Data they access and process.

3. Privacy compliance programs and accountability

Data Privacy Managers define, implement and monitor privacy compliance programs.to ensure efficient and continuously improving management of Data Protection.

Accountability is the founding principle of in particular the European Regulation. The Entities (as Data Controllers or Data Processors) must implement all appropriate and effective measures, be in a position to demonstrate that Data Processing are compliant and the effectiveness of the measures taken.

The implementation of the present Policy is one of the essential components of the Group's commitment to the protection of Personal Data, and of the Accountability for achieving compliance with the European Regulation and other local legislation.

4. Data protection means and principles

1. Awareness and training

All personnel must be made aware of the issues involving Data Privacy.

2. Reviews, Risk and Audits

Concerning the Internal Control, a Data Protection referential is managed by the Group DPM. It is a set of key controls to be implemented according to a Group scope defined by the Group DPM on a risk-based approach. DPMs / DPOs of the organization are responsible to perform an annual self-assessment to confirm the effectiveness of these key controls, and define improvement actions if needed.

The Enterprise Risk Management exercise is prepared by the Group DPM in coordination with the Risk Management Department. It is the responsibility of the DPMs / DPOs of the organization to conduct the exercise and implement the necessary action plans.

The effective conduct of these actions can be subject to audits conducted by the Internal Audit Department.

3. Data Process mapping

It is recommended that each Entity of the organization establishes a map and a register[2] of all significant Data Processing to offer a comprehensive overview and allow for the Data Processing to be controlled and rationalized as well as to facilitate the Data Controller's handling of the Data Subject's access request.

4. Incident Handling

Any person being aware of an inappropriate use of Personal Data will contact their DPM / DPO who will report this incident to his Ethics Officer. Data Privacy Managers are informed of data breaches and act on them in cooperation with Chief Information Security Officers.

DPMs / DPOs on the GDPR scope will have to notify, where required, data breaches to their Supervisory Authority within the timeframe indicated by their local legislation and, if necessary, notify the affected Data Subjects.

5. Written agreements

Written agreements must be established between the parties concerned by the implementation of a Data Processing (ENGIE, its clients or partners). Under all circumstances, the collection, use or subcontracting of Personal Data must comply with the laws in force, the ENGIE Ethics Charter and the present Policy.

[2] For some Entities, the register is an obligation, according to local legislation, such as European Regulations. .

Other protection principles are required to be implemented within ENGIE (unless national laws are contrary to or more stringent) :

1. Explicit, legitimate, fair and transparent purposes
2. Relevance, minimization and proportionality of collected data
3. A limited retention period
4. Sensitive Data, sensitive files and processing at risk
5. Confidentiality and Security obligations
6. Classification and Protection of Personal Data
7. Upstream risk process (Privacy by Design, by Default, Data Privacy Impact Assessment)
8. International Transfers
9. Openness and respect for individuals' rights (Information notice, consent, access rights, …)
10. Data Processors obligations