

Dated

15th of January 2015

ENGIE BINDING CORPORATE RULES

validated by the European Data Protection Authorities

Contents

	Page
1 Introduction.....	1
2 Definitions.....	1
3 Scope of the BCR and relations with applicable national laws	3
4 Principles governing the Processing and transfers of Personal Data	4
5 Information and rights of the Data Subjects	8
6 Third party beneficiary rights	9
7 Training	10
8 Governance and Auditing of BCR's application	10
9 Complaints Procedure.....	10
10 Liability	11
11 Cooperation with Data Protection Authorities	12
12 Applicable law	12
13 Contact	12

validated by the European Data Protection Authorities

1 Introduction

Mindful of the importance of Data Privacy, the ENGIE¹ Group is committed to protecting the Data Subjects' Personal Data and ensuring compliance with the Data Privacy regulations applicable in the countries where the ENGIE Group is present.

To this end, the ENGIE Group has already established uniform and appropriate data protection standards for the Processing of the Data Subjects' Personal Data through the adoption on the 20th of January of 2014 of the Group Data Privacy Policy.

The purpose of these Binding Corporate Rules ("BCR") is to supplement the Group Data Privacy Policy and the Ethical Charter in order to ensure an adequate level of protection for the transfers and related Processing of the Data Subjects' Personal Data within the ENGIE Group and to facilitate Group-wide transfers, in compliance with the applicable legal requirements, in particular those set out in the EU Directive 95/46/EC dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

All entities within the ENGIE Group and their managers, officers and employees undertake to comply with and at all times respect these BCR when collecting, using, transferring and otherwise Processing Personal Data relating to a Data Subject.

2 Definitions

For the purpose of these BCR, the terms and expressions used with a capital letter shall have the meanings ascribed to them below, being specified that irrespective of the definitions below, the terms of these BCR shall in any event be construed in accordance with the applicable European legislation, namely at the date of execution of these BCR, the EU Directive 95/46/EC of 24 October 1995:

"Data" or **"Personal Data"** shall mean any information relating to an identified or identifiable individual. An individual is considered identifiable, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data subject to these BCR are "HR Data" as this term is defined below.

- **"HR Data"** shall mean any Personal Data relating to Data Subjects in the sense of staff members, i.e. employees, candidates, trainees, temporary workers, or retirees of any ENGIE Affiliate;

¹ Formerly GDF SUEZ

“Data Controller” or **“Controller”** shall mean the individual or legal entity, public authority, agency or any other body which solely, or jointly with others, determines the purposes and means of Personal Data Processing.

“Data Exporter” or **“Exporter”** shall mean the EEA based Data Controller who transfers Personal Data.

“Data Importer” or **“Importer”** shall mean, as the context requires: (i) the Data Controller who agrees to receive from the Data Exporter Personal Data for further Processing in accordance with the terms of these BCR or (ii) the Data Processor who agrees to receive from the Data Exporter Personal Data intended for Processing on behalf of Data Exporter after the transfer in accordance with his/her instructions and the terms of these BCR.

“Data Privacy Officer” (**“DPO”**) shall mean the individual appointed by a ENGIE Affiliate or a ENGIE Business Line as the person advising the Data Controller and monitoring compliance with Data Protection laws.

“Data Processing” or **“Processing”** or **“Processed”** shall mean any manual and/or automated operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collecting, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing by means of transmission, dissemination or otherwise making available or transferring, alignment or combination, blocking, deletion or removal. Data Processing and their related purposes falling within the scope of these BCR.

“Data Processor” or **“Processor”** shall mean the individual or legal entity, public authority, agency or any other body who processes Personal Data on behalf of Data Controller.

“Data Protection” or **“Data Privacy”** shall mean the set of actions, activities, methods, processes, organizations and so forth aiming at protecting Personal Data and ensuring compliance with applicable Data Privacy laws and regulations.

“Data Protection Authority” shall mean a national independent authority notably in charge of monitoring the compliance with applicable data protection laws in its country. A list of the existing Data Protection Authorities is available at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

“Data Subject” shall mean an identified or identifiable individual whose Personal Data is concerned by Processing, regardless his/her nationality.

“EEA” shall mean the European Economic Area.

“ENGIE Affiliate(s)” shall mean legal entities within the consolidated scope of the Group (global integration).

“ENGIE Group” shall mean ENGIE SA and all of ENGIE Affiliates.

“ENGIE Group Data Privacy Policy” shall mean the principles and objectives, the organization and monitoring system that have been implemented together with the roles and responsibilities with regard to personal data protection.

“Group Data Privacy Officer” shall mean the individual appointed at ENGIE SA, in charge of Data Privacy at the ENGIE Group level to define and spread good practices relating to Data Privacy and to ensure their implementation.

“Sensitive Data” shall mean any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, as well as Data concerning health or sex life.

“Third Party” shall mean any individual or legal entity other than Data Subjects including any public authority, agency or any body other than ENGIE SA and the ENGIE Affiliates.

3 Scope of the BCR and relations with applicable national laws

- 3.1 These BCR aim at ensuring an adequate level of data protection and providing for adequate data protection safeguards within the meaning of Articles 25 and 26 of the EU Directive 95/46/EC of 24 October 1995 (“the EU Directive”) across the ENGIE Group.
- 3.2 These BCR thus apply to any and all transfers and Processing of the Data Subjects’ Personal Data within the ENGIE Group, which are or have been subject to the EU Directive, and more specifically, to all Data Subjects’ Personal Data:
- collected and Processed in the European Economic Area (EEA) zone by ENGIE SA and/or any of ENGIE Affiliates headquartered in the EEA;
 - Processed by any of ENGIE Affiliates headquartered out of the EEA zone, insofar as the Personal Data is collected in the EEA .
 - collected out of the EEA zone by any of ENGIE Affiliates headquartered out of the EEA and transferred or otherwise made available by the collecting recipient to ENGIE SA and/or any of ENGIE Affiliates headquartered in the EEA.
- 3.3 These BCR do not cover Personal Data Processed exclusively out of the EEA zone. In the event that local law requires a higher level of protection of Personal Data, therefore the applicable local law will take precedence over the BCR. In the opposite case where local law provides a lower level of protection of Personal Data than the protection provided by these BCR, in such case, the provisions of the BCR shall apply.

3.4 Binding character of the BCR upon entities and employees:

These BCR shall apply to all Entities of ENGIE Group having signed the Group-wide Agreement providing for their acceptance of the BCR and shall be binding on every said Entity and its respective employees. For this purpose, each Entity shall ensure the enforcement of these BCR, by the compliance with the Group Code of Ethics and when required one or several of the following schemes to be implemented in accordance with the applicable labor legislation:

- the internal rules,
- a provision of the employment contract,
- any other provision aiming at making the BCR enforceable on its employees.

4 Principles governing the Processing and transfers of Personal Data

4.1 In order to provide the Data Subjects with an equivalent and adequate level of protection throughout the ENGIE Group within the meaning of Articles 25 and 26 of the EU Directive 95/46/EC of 24 October 1995, ENGIE SA and ENGIE Affiliates undertake to apply and strictly comply, and shall procure that the respective managers, officers and employees, shall apply and strictly comply to the principles set out below when Processing and transferring Personal Data as this term is defined hereinabove:

(a) Lawfulness and fairness of Processing and legitimacy of Processing purposes

Personal Data must be collected, transferred and otherwise Processed by fair means and in a lawful manner, i.e. in a transparent manner, and for specified, explicit and legitimate purposes. Personal Data must not be used, transferred or otherwise Processed subsequently, including by Importers acting as Data Controller, in a way that is incompatible with the initial purposes.

Consequently:

- (i) the Data Subject must be provided with all information required under applicable national data protection laws in relation to the Processing of his/her Personal Data,
- (ii) when required under the relevant local Data Protection law, the Processing must be notified to the competent Data Protection Authority; and
- (iii) the Processing of the Personal Data must rely on a legal ground, such as:
 - the Data Subject's explicit consent to the Processing; or,

- the compliance with a legal obligation to which the Data Controller is subject; or,
- the performance of a contract to which the Data Subject is party or prior to entering into a contract at the Data Subject's request; or,
- the protection of the Data Subject's vital interests; or,
- the performance of an assignment carried out in the public interest or in the exercise of an official authority vested in the Data Controller or in the recipient(s) of the Personal Data; or,
- the achievement of the Data Controller's or the Data recipient's legitimate interest, provided this is not incompatible with the Data Subject's interest or fundamental individual rights and freedoms.

(b) Relevance and proportionality of Personal Data Processed

The Personal Data collected, transferred or otherwise Processed must be adequate, relevant and not excessive with respect to the purposes for which it is collected and further Processed. The Personal Data must be accurate, comprehensive and updated if need be.

The retention period of the Processed Personal Data must be defined in accordance with the intended purpose of Personal Data collecting, transferring and Processing. The Personal Data shall be stored in a form that allows the identification of related Data Subjects for a period of time no longer than that is necessary with respect to the purposes for which it is collected and further Processed.

When the collecting Personal Data is no longer needed for the purpose of its Processing, said Personal Data must be deleted or made anonymous, as required under applicable local Data Protection laws.

(c) Additional safeguards applicable to Sensitive Data

Sensitive Data shall not be collected, transferred and/or otherwise Processed unless this Processing is made on a legal basis, namely:

- (i) the Data Subject has given his/her express and explicit consent (except where prohibited under the applicable local law); or,
- (ii) the circumstances under which Sensitive Data must be collected, transferred and/or otherwise Processed are specifically allowed by the applicable local law, it being the case notably when:

- the Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller in matters of labour law insofar as it is authorized by local law providing for adequate safeguards;
- the Processing is necessary to protect Data Subject's or another person's vital interests in the case where the Data Subject is physically or legally unable to give his/her consent; or
- the Processing relates to Personal Data which is obviously made public by the Data Subject;
- the Processing is necessary for the filing, exercise or defence of a legal claim; or,
- the Processing is carried out in the course of its legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union purpose, subject to appropriate guarantees given thereto and provided that the Processing relates solely to the members or individuals having regular contact therewith and the Personal Data is not disclosed to a Third Party without the Data Subject's explicit consent; or
- the Processing of the Sensitive Data is required for the purposes of preventive medicine, medical diagnosis, the providing of care or treatment or health-care services, and in places where said Sensitive Data is processed by a health professional or any other individual bound by the obligation of professional secrecy or an equivalent obligation of secrecy under the laws or rules of relevant authorities.

(d) Specific rules applying to automated individual decisions

Under no circumstances, an evaluation of or a decision about the Data Subjects which significantly affects them shall be based solely on automated Processing of their Personal Data unless that decision:

- (i) is taken in the course of the entering into or the performance of a contract, provided the request for the entering into or the performance of the contract, made by the Data Subject, has been satisfied or provided that appropriate actions are taken to safeguard his/her legitimate interests, such as arrangements allowing him/her to provide his/her comments; or

- (ii) is authorized by a law which also lays down measures to safeguard the Data Subject's legitimate interests.

(e) Confidentiality and Security obligations

The ENGIE Group shall protect the Data Subjects' Personal Data against incidental unauthorised access, unlawful Processing, accidental or unlawful disclosure, loss, destruction or damage caused thereto. Consequently, ENGIE Group undertakes to implement protective actions and in particular, material, technical and organizational security measures aimed at adequately safeguarding the security and the confidentiality of the Data Subjects' Personal Data.

These measures depend on the existing risk, the potential consequences on the Data Subject, the level of sensitivity of the Personal Data, the available technology and the state of the art in the jurisdictions of ENGIE SA or any of ENGIE Affiliates.

(f) Data transfers to Data Processors

Whenever ENGIE or any of ENGIE Affiliates, acting as Data Controller, uses a Data Processor for the Processing of Data Subjects' Personal Data, whether in or out of the scope of ENGIE Group, said ENGIE Affiliate must procure that, prior to the transfer of Personal Data to any Data Processor, the selected Data Processor offers sufficient guarantees in respect of technical security measures and organizational measures governing the Processing, and must procure that the selected Data Processor complies with those measures.

Consequently, the contract to be concluded with the selected Data Processor will include a clause by which the Data Processor shall act only on instructions given by the Data Controller and shall implement the rules for security and confidentiality safeguarding incumbent on the Data Processor.

(g) Restrictions on transfers and onward transfers to a Data Controller being out of ENGIE Group

In all transfers and subsequent transfers of Personal Data to a Third Party acting as a Data Controller headquartered out of the EEA zone, the contract with said Data Controller shall include the latest EU standard contractual clauses approved by the European Commission governing transfers of Personal Data by one Data Controller to another Data Controller and shall be signed by all involved parties, unless the transfer is under a legal exemption pursuant to applicable local data protection law or unless the transfer is made to a Data Controller being in the scope of a US Safe Harbour certification in matters of Personal Data transfer or is headquartered in a country recognized by the European Commission as offering an appropriate level of protection. In any event, such transfers

shall comply with the EU Directive 95/46/EC of 24 October 1995, in particular its articles 25 and 26 on trans-border data flows.

5 Information and rights of the Data Subjects

5.1 Information of the Data Subjects

- (a) In order to ensure that all involved Data Subjects are informed of the existence and content of these BCR and in addition to the training sessions which will be provided to the employees of the ENGIE Group as set out in Article 7 below, each entity of ENGIE Group undertakes to
 - (i) communicate these BCR (including any updates thereof) to all employees of their own Business Unit notably by means of Intranet and by internal memo and
 - (ii) make these BCR available at least on ENGIE website on the following address: www.engie.com.
- (b) Each entity of ENGIE Group also undertakes to provide the Data Subjects, prior to any Processing of their Personal Data, with any information as this may be required under applicable local data protection law and in any event, with the following set of information *a minima*:
 - (i) the Data Controller(s)' and of its representative(s)' identity, if any;
 - (ii) the intended purposes of the Personal Data Processing; and,
 - (iii) insofar as such information is necessary, in consideration of the specific circumstances requiring Personal Data collecting, the guarantee of fair processing in respect of Data Subject, and any further information such as:
 - the recipients or categories of recipients to which Personal Data is addressed,
 - the existence of a right of access to and a right to amend his/her Personal Data as further described in Article 5.2 below.
- (c) Such information may be made available to the Data Subject on ENGIE website and/or on any relevant ENGIE Affiliate website, and/or in appropriate policies and charters, and/or in contracts concluded with Data Subject being involved in the Processing of the Data Subject' s Personal Data and/or by any other appropriate means (correspondence, information notice, etc).

- (d) In the event that Personal Data is not provided directly by the relevant Data Subject, the obligation to inform the Data Subject will not apply insofar as such information proves to be impossible or to involve a disproportionate effort in this respect or if the recording or the disclosure is expressly permitted by applicable local law(s).

5.2 **Right of access, amendment, erasure, blocking of and objection to Personal Data**

Each entity of ENGIE Group shall grant the Data Subjects with the following Data Subjects' rights:

- (a) to obtain without constraints, at reasonable intervals, and without excessive delay or expense, a copy of their Personal Data being processed;
- (b) to obtain the amendment, erasure or blocking of their Personal Data, in particular when their Personal Data are incomplete or inaccurate;
- (c) to object, at any time and on compelling relevant legitimate grounds, to the Processing of their Personal Data, unless said Processing is required by law. Where the objection is justified, the Processing must be stopped;
- (d) to object, on request and free of charge, to the Processing of their Personal Data for direct marketing purposes.

The above rights can be exercised by Data Subjects pursuant to the procedure provided in the information notice given by ENGIE SA or any of the relevant ENGIE Affiliate involved in the Processing.

6 **Third party beneficiary rights**

Data Subjects who have suffered a damage due to a breach of these BCR may, as third party beneficiaries of these BCR, exercise their rights in pursuance of these rules and take their case either to the competent Data Protection Authority or the Court where the EEA Exporting Affiliate is headquartered.

The principles that may be enforced by Data Subjects are the following:

- Lawfulness and fairness of Processing and legitimacy of Processing purposes;
- Relevance and proportionality of Personal Data Processed;
- Additional safeguards applicable to Sensitive Data;
- Specific rules applying to automated individual decisions;

- Confidentiality and Security obligations;
- Specific rules applying to Data transfers to Data Processors or on transfers and onward transfers to a Data Controller being out of the ENGIE Group;
- Transparency and easy access to the BCR;
- Rights of access, rectification, erasure, blocking of data and objection to the processing;
- Rules in case a national legislation prevents compliance with the BCR;
- Right to complain through the internal complaint mechanism;
- Duty to cooperate with Data Protection Authorities;
- Liability rules and third-party beneficiary rights.

7 Training

- 7.1 All personnel within the ENGIE Group and more particularly, those who have permanent or regular access to Personal Data, or are involved in Personal Data collecting, in the development or acquisition of tools used for Personal Data Processing, must be formally informed of the content of these BCR and more generally, of the issues raised, i.e. legal and security issues.
- 7.2 Therefore, Global awareness campaigns and appropriate training sessions will be conducted by ENGIE SA at ENGIE Group level. Local actions will also be carried out by ENGIE Affiliates in addition to these campaigns and training sessions.

8 Governance and Auditing of BCR's application

9 Complaints Procedure

9.1 Data subjects

- (a) **Complaint:** if a Data Subject makes any complaint on the handling of his/her Personal Data under the BCR, or if a Data Subject has a reasonable ground to suspect that his/her Personal Data is Processed unlawfully under local data protection legislation, he/she may raise the matter with either his/her legal entity DPO, or, if no DPO is in place at entity level, with his/her Business Unit DPO, or, if no DPO is in place at Business Unit level, with his/her Business Line DPO.

Complaints should be made by Email and copied to the appropriate relevant DPO.

Candidates or retired employees to which these BCR apply, shall send their complaints by email at privacy@engie.com.

If the complaint of the Data Subject is rejected and if the Data Subject is not satisfied with the way in which the complaint has been dealt with, he/she has the right to lodge a complaint with an EEA or a national data protection authority with competent jurisdiction and/or to take action to a competent state court to enforce his/her rights under the BCR.

(c) Direct complaint

A Data Subject remains in any case entitled to lodge a claim directly before an EEA or national data protection authority with competent jurisdiction and/or before a competent state court, without using the internal complaint proceedings as described in the previous paragraphs.

10 Liability

10.1 Liability principles

Exporters and Importers of Personal Data are liable for breach of their respective obligations towards the Data Subjects in accordance with the principles set out in this article 10. They shall exclusively carry out the burden of proof in this respect and may therefore only be either partially or fully exonerated if they can prove that they have no responsibility in the cause of the damage.

10.2 Where the Importer is a Data Controller

Where the Importer has received the Personal Data for Processing for its own purposes as Data Controller, the Importer and the Exporter shall be liable to the Data Subject in accordance with the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries attached to the European Commission Decision 2001/497/CE.

Any Data Subject, who suffered damage as a result of any breach of the obligations arising out of the BCR by an Exporter or an Importer, shall have the right to enforce his/her rights in the jurisdiction of the Exporter's country of establishment and is entitled to receive compensation either from the Exporter, or from the Importer, for the damage suffered,

10.3 Where the Importer is a Data Processor

Where the Importer has received the Personal Data as a Data Processor, the Exporter shall be liable to the Data Subject in accordance with the sections (i) and (ii) below corresponding to the liability clause (Clause 6) of the Standard Contractual Causes for the Transfer of Personal Data to Data Processors in Third Countries in accordance with the European Commission Decision 2010/87/EU.

- (i) Any Data Subject, who suffered damage as a result of any breach of the obligations arising out of the BCR by an Exporter or an Importer, is entitled to receive compensation from the Exporter for the damage suffered.
- (ii) However, if the Exporter is wound up factually or ceased to exist in law or has become insolvent, the Importer agrees that the Data Subject may issue a claim against the Importer as if it were the Exporter, unless any successor legal entity has assumed the entire legal obligations of the Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity at the place of jurisdiction of the Exporter.

11 Cooperation with Data Protection Authorities

The ENGIE Group undertakes to (and procures that all members of the ENGIE Group will) cooperate with the Data Protection Authorities, notably in the context of audits or investigations by these Authorities and, considerate any advices and recommendations of the Data Protection Authorities on any issues regarding these BCR.

12 Applicable law

These BCR are governed by French law.

13 Contact

Data subject can raise any concerns with the ENGIE Group Data Protection Officer.

ENGIE
Group Data Protection Officer
Mail box 28.12
1 Place Samuel de Champlain
92930 Paris la Défense
FRANCE