Dated **15th of January 2015**

ENGIE BINDING CORPORATE RULES

Contents

1 Introduction

ENGIE SA[1] ("ENGIE SA") and the ENGIE[2] entities listed in Appendix 1 as amended from time to time ("ENGIE Affiliates") (together "ENGIE Group") are required, in the course of their business activities, to process Personal Data relating to their employees and other assimilated personnel (such as candidates, etc), ("Data Subjects").

Mindful of the importance of Data Privacy, the ENGIE 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 (see Appendix 2).

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 both 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, and the EU Directive 02/58/EC dated 12 July 2002 as amended concerning the processing of personal data and the protection of privacy in the electronic communications sector.

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.

These BCR are communicated to all the employees of the ENGIE Group [notably through the Intranet and by internal memo] and are available on ENGIE website at the following address: www.engie.com.

For any questions with respect to these BCR, or to your rights under the BCR or any other privacy issues, please contact the Group Data Privacy Officer at the address below:

privacy@engie.com.

[1] ENGIE SA is the new legal corporate name

[2] ENGIE is the new name of GDF SUEZ

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;

"**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 Committee**" ("**DPC**") shall mean the Committee set up under ENGIE Group Data Privacy Policy with the purpose to conduct activities to promote and/or to ensure the application of ENGIE Group Data Privacy Policy.

"**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 are further provided in Appendix 3.

"**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, organisations 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) as set forth in Appendix 1 attached hereto as may be amended from time to time pursuant to Article 13 below.

"**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, as attached in Appendix 2.

"**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 as defined in Appendix 1, for all categories of Personal Data and all related transfers and Processing as further described in Appendix 3 in accordance with the purposes as set out in said Appendix.

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 and further transferred or made available by ENGIE SA and/or any of ENGIE Affiliates headquartered in the EEA to any of ENGIE Affiliates headquartered out of 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 for Processing, whether or not such Processing occurring in the EEA zone involves subsequent transfer back of Personal Data to the collecting recipient headquartered out of the EEA.

These BCR do not cover Personal Data Processed exclusively out of the EEA zone. The Processing of Personal Data collected out of the EEA by any of ENGIE Affiliates headquartered out of the EEA, with no further transfer to the EEA, whether in whole or in part, is subject to national data protection law applicable in the place where the data is Processed only.

3.3 Each Exporter and/or Importer in ENGIE Group shall procure that the transfers and Processing of the Data Subjects' Personal Data comply with these BCR and, in any event, with the applicable law as provided by Article 4 of the EU Directive 95/46/EC of 24 October 1995 and any relevant local laws. Each Exporter and/or Importer shall undertake, when Personal Data includes Sensitive Data, to provide additional safeguards similar to those provided by the EU Directive 95/46/EC of 24 October 1995, as further described in Article 4.1(c) below.

3.4 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.

3.5 If a ENGIE Affiliate has reasonable ground to believe that the applicable local law prevents it from fulfilling its obligations under these BCR and will adversely affect the guarantees provided hereunder to Data Subjects, it shall immediately inform ENGIE SA and the Group Data Privacy Officer, except where prohibited by a law enforcement authority. In such circumstances, ENGIE SA and/or the Group Data Privacy Officer will take a responsible decision as to the action to carry out and will consult the relevant Data Protection Authority in case of any doubt.

3.6 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. Appendix 1 is reflecting the list of Entities for which approval of BCR is sought.

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 and provided as an indication in Appendix 3.

(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, as further described in Article 5.1 below;

(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 effects 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.

The security measures implemented at the ENGIE Group level are notably defined in the ENGIE policies and security standards relating to the Information Systems as set forth in Appendix 4.

Security incidents shall be handled in accordance with the rules provided in Group Data Privacy Policy.

(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 similar to the standard clause provided in Appendix 5 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.

When the Data Processor is headquartered out of the EEA zone and is not a ENGIE Affiliate, the contract with said Data Processor shall include the latest EU standard contractual clauses approved by the European Commission, governing transfers of Personal Data by a Data Controller to a Data Processor, unless the transfer is under a legal exemption pursuant to applicable local data protection law or unless the transfer is made to a Data Processor 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.

(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 Processed 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 in accordance with Article 10 below.

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

- Lawfulness and fairness of Processing and legitimacy of Processing purposes (see article 4(a) above);
- Relevance and proportionality of Personal Data Processed (see article 4(b) above);
- Additional safeguards applicable to Sensitive Data (see article 4(c) above);
- Specific rules applying to automated individual decisions (see article 4(d) above);
- Confidentiality and Security obligations (see article 4(e) above);
- 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 (see article 4(g) and 4(f) above).
- Transparency and easy access to the BCR (see article 5.1 of GDF BCR) ;
- Rights of access, rectification, erasure, blocking of data and objection to the processing (see article 5.2);

- Rules in case a national legislation prevents compliance with the BCR (see article 3.5);

- Right to complain through the internal complaint mechanism (see article 9);

- Duty to cooperate with Data Protection Authorities (see articles 8.2(a)(v); 8.2(b)(iv); 8.2(c); and 12);

- Liability rules and third-party beneficiary rights (see articles 6 and 10).

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 Global awareness campaigns and appropriate training sessions (on site or through webinars) 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.

7.3 Specific training of Data Privacy Officers will be conducted according to the same principles.

7.4 All these actions, whether at the Group or at a local level, must be coordinated by the Group Data Privacy Officer and the local Data Privacy Officer(s).

8 Auditing of BCR's application

8.1 Governance

(a) At ENGIE Group's level

The strategic management of these BCR is the responsibility of ENGIE General Management Committee, while the coordination and operational management of the BCR is delegated to the Group General Secretary. The Group General Secretary delegates this responsibility to the Group Data Privacy Officer.

Any difficulty in implementing these BCR must be addressed to the Group Data Privacy Officer.

(i) The Group Data Privacy Officer

The Group Data Privacy Officer is mainly in charge of the following:

- monitoring the compliance with these BCR and any applicable binding policy, including the Group Data Privacy Policy, and advising/alerting the Board of Management of any related risks;

- receiving notification from the DPOs of Data Subjects' complaints and to handle major privacy issues;

- reporting on the compliance status of these BCR on an annual basis to the Data Privacy Committee;

- representing ENGIE Group in this matter with external stakeholders and organizations, including in the context of Data Protection Authorities' investigations;

- coordinating the management and handling of incidents relating to Data Protection pursuant to the rules provided by the Group Data Privacy Policy.

(ii) The Data Privacy Committee

The Data Privacy Committee (DPC) as defined in Appendix 2 – ENGIE Group Data Privacy Policy - shall meet twice a year on BCR's matters.

The DPC decides upon local or transversal actions and submits them for approval to the Group level authorities, and/or to the ENGIE General Management Committee if need be.

Once a year, the DPC shall carry out a review of its activities (including an update on the application of these BCR and the Group Data Privacy Policy) and shall give a presentation thereof to the relevant Group level authorities.

(b) At Business Line's and Business Unit's levels

Each Business Line (and where appropriate, Business Units) shall appoint a Data Privacy Officer (DPO) who coordinates the activities relating to Data Protection within his/her area of competence.

The DPO's assignments are the following:

- monitoring the implementation and the compliance of the BCR and the Group Data Privacy Policy in the Business Line (or Business Unit);

- informing, advising and alerting Data Controllers on Data Protection issues;

- representing its BL or BU in this matter with external stakeholders and organizations, including in the context of Data Protection Authorities' investigations;

- handling local complaints made by Data Subjects pursuant to Article 9 below and addresses them to the Group Data Privacy Officer;

- taking part in the awareness campaigns and training sessions among the staff of the Business Line or Business Unit;

- participating in the activities organized by the Group Data Privacy Officer (in matters of good practices, feedback from past experience, etc.) and is an active member of the network;

- reporting on key events on an annual basis;

- reporting on any incident such as an inappropriate use of Personal Data or a security incident to the Ethics Officer pursuant to the rules provided in the Group Data Privacy Policy.

(c) At legal Entity's level

Each ENGIE Affiliate shall procure that these BCR and the Group Data Privacy Policy are complied with prior to any action of Data Processing, during the course of its execution and operation.

When required by law, the DPO (or an individual so-appointed) shall be in charge of the compliance with local data protection laws requirements, such as the fulfilment of the formalities filings with the relevant national Data Protection Authorities.

8.2 Control and Audit

(a) Internal Control

(i) The ENGIE Group has implemented an Internal Control program whereby most significant ENGIE Affiliates, i.e. contributing to more than 85% of the Group turnover, shall report on their compliance to a framework of controls corresponding to the internal and external regulations on a yearly basis; other Affiliates contributing to less than 85% of the Group turnover shall nevertheless be involved in the yearly internal Control as soon as they start transferring Personal Data.

(ii) The Group Data Privacy Policy is included in the framework of controls monitored through the Internal Control Program.

(iii) These controls cover all aspects of the BCR, notably:

- Organization;
- Procedures;
- transparency and fairness with respect to Data Subjects;
- limitation of Processing purpose;
- ensuring of Personal Data quality;
- ensuring of individual rights of access, amendment and objection to Processing;
- confidentiality and security measures;
- limitation of the period of time of Data storing.

The above list may be extended.

(iv) As part of the Internal Control program, the Operational manager (or business process owner) within the affiliate must conduct an assessment of the efficiency of the controls, on an annual basis.

(v) The results of these assessments and the proposed corrective actions are communicated to the management and to the Group Management, if need be. The relevant DPO(s) and Group Data Privacy Officer must be informed thereof. The Data Protection Authorities may be provided with these results, upon request made to the Group Data Privacy Officer.

(b) Internal Audits

(i) Upon request of the Management (at the level of the Group, the Business Line, the Business Unit or the Affiliate), ENGIE Internal Audit teams shall perform audit assignments on specific matters of interest, such as legal entities, risks or operational processes and onward transfers of Personal Data. In addition to these specific assignments, Internal Audit teams are vested with the responsibility of auditing the efficiency of the Internal Control program.

(ii) All aspects of the Internal Control are covered by Internal Audit, in particular :

- The relevance of the framework of controls with regards to the regulations

- The scope of application (ENGIE Affiliates requested to participate)
- The relevance of the controls implemented at operational level
- The assessment performed by the Operational Manager according to .8.2.a.iii and iv and the efficiency of such assessment
- The corrective actions taken (if any)

(iii) The auditing of Internal Control by Internal Audit is carried out on a yearly basis at Group Level and every 5 to 7 years as an average at operational level.

(iv) The results of these assessments and the proposed corrective actions are communicated to the management and to the Group Management, if need be. The relevant DPO(s) and Group Data Privacy Officer must be informed thereof. The Data Protection Authorities may be provided with these results, upon request made to the Group Data Privacy Officer.

External Audits

(i) ENGIE SA and each ENGIE Affiliate are informed hereby that the Data Protection Authorities are empowered by applicable laws to carry out audits if need be, and consequently, hereby accept that they can be audited in this respect by the relevant Data Protection Authorities and hereby undertake to abide by the rulings of the Data Protection Authorities on any issue related thereto.

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.

This Data Privacy Officer shall:

(i) notify the Group Data Privacy Officer thereof;

(ii) initiate an investigation; and

(iii) when necessary, advise the most significant affiliates on the appropriate measures to ensure the compliance with and the monitoring of, through to completion, including the actions designed to permit the compliance therewith.

(b) **Reply to the Data Subject:** within one month of receipt of the complaint, the Data Privacy Officer of the Data Subject legal entity (if any), or the Business Line or Business Unit Data Privacy Officer shall inform the Data Subject in writing of ENGIE's position with regards to the complaint and any action undertaken or to be undertaken by ENGIE in remedy of the prejudice or, in case the relevant Data Privacy Officer is not able to give ENGIE's position within one month, he/she shall inform the Data Subject of the date when the Data Subject will receive notice of ENGIE's position on this issue, the date of which shall be no later than two months after receipt of the complaint. The relevant Data Privacy Officer shall send a copy of the complaint and his written reply to the Group Data Privacy Officer.

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 Binding Corporate Rules.

(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.

9.2 Common rules

(a) Within the framework of these BCR, the Data Privacy Officers are responsible for:

- identifying and registering individual complaints from Data Subjects,
- drawing up a list of such complaints,
- conducting an enquiry into the reality of the alleged contraventions,
- seeking to mediate by offering compensation, after informing the Group Data Privacy Officer. There is a systematic mediation and amicable settlement procedure before matters are referred to court or the supervisory authority with jurisdiction.

(b) The independence of Data Privacy Officers is guaranteed during the performance of their duties and they are bound to strict neutrality and impartiality in the cases they handle.

(c) The identity of the Data Subject, the content of the complaint and the identity of the entity shall be kept confidential.

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.

10.4 Liability principles between the Exporters and Importers

In the relations between Exporters and Importers, each Affiliate shall be liable to the other Affiliates for damages it causes by any breach of the BCR, the liability being limited to the actual damage caused. In this respect, if one Affiliate is held liable for a breach by another Affiliate, the latter shall, to the extent to which it is liable, indemnify the first Affiliate; e.g., if an Importer is in breach with the BCR and the Exporter compensates the Data Subject with regards to such breach, then the Importer shall indemnify the Exporter. Similarly, if an Exporter is in breach with the BCR and the Importer compensates the Data Subject with regards to such breach, the Exporter shall indemnify the Importer.

10.5 Each Affiliate hereby formally acknowledges its above-described liabilities with respect to Data Subjects.

10.6 The Affiliates ensure that they have sufficient financial means to compensate the Data Subjects for the damage caused as a result of unlawful Data Processing under the BCR.

11 Internal actions

In case an Affiliate breaches these Binding Corporate Rules, fails to apply the recommendations and advice issued after the Privacy Officers have checked for compliancy, or fails to cooperate in BCR compliance auditing carried out by Data Privacy Officers or by the relevant Data Protection Authorities, and if requested by the Group Data Privacy Officer, following measures may be taken by ENGIE SA:

- publication of the Privacy Officer's recommendations on the Group's intranet,
- publication of the sanctions decided by the Data Protection Authority,
- temporary or definitive ban on continued data flow.

12 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.

Such cooperation will notably consist in:

- having the necessary personnel available for dialogue with the relevant Data Protection Authority/Authorities;

- reviewing in an active way and considering any decisions made by any Data Protection Authority having jurisdiction on data protection law issues that may affect these BCR;

- assisting any audit or investigations conducted by a Data Protection Authority as set out in Article 8.2 (c) above;

- undertaking to abide by any formal and final decision of a Data Protection Authority having jurisdiction on any issue relating to the construction or application of these BCR.

13 Updating the BCR

13.1 The Data Privacy Committee is solely entitled to decide any amendment to these BCR.

13.2 The Data Privacy Committee will appoint a team or an individual in charge of keeping up to date the list of the ENGIE Affiliates attached hereto in Appendix 1.

13.3 Any significant changes to these BCR or to the list of the ENGIE Affiliates shall be notified by ENGIE SA to the relevant Data Protection Authorities , it being provided that:

(a) some of these changes might require a new authorization from the Data Protection Authority;

(b) updates to the BCR or to the list of the ENGIE Affiliates are possible without applying for an authorization providing that:

(A) an identified individual keeps a fully updated list of the members of the BCR and keeps track of and records any updates to the BCR and provides the necessary information to the Data Subjects or Data Protection Authorities upon request;

(B) no transfer is made to a any newly formed ENGIE Affiliate or existing ENGIE Affiliate, which has not yet adhered to the BCR, until such ENGIE Affiliate is expressly bound by the BCR and undertakes to comply therewith;

(C) any changes to the BCR or to the list of the ENGIE Affiliates is reported once a year to the relevant Data Protection Authority with a brief explanation of the reasons justifying the update.

13.4 These BCR will specify the date on which the BCR are last reviewed and the date of revisions thereof.

14 Contractual documents

The contractual documents are the following documents listed by decreasing order of precedence:

1. These BCR;
2. The Appendices to these BCR;
3. The Group-wide Agreement signed by each Entity of the ENGIE group.

Such order of precedence shall be applied and BCR shall always prevail in case of conflict or inconsistency.

15 Applicable law

These BCR are governed by French law.

16 Effective date – Duration

These BCR shall enter into effect on [_____] , for an indefinite term.

Appendix 1 : List of Entities for which approval of the BCR is sought

Périmètre GDF SUEZ
sociétés en intégratio

Appendix 2: GDF SUEZ Group Data Privacy Policy

GDF SUEZ DECISION

Date: 31st of January 2014

Reference: GDF SUEZ 2013 – 005

Issuer: General Secretariat

Contact: Jacques PERRET jacques.perret@gdfsuez.com Tel.: +33 (0)1 44 22 50 17

Group Data Privacy Policy

Summary

This decision describes the GDF SUEZ Group Data Privacy Policy applicable to all Entities of the Group. Where necessary due to local regulations, this policy may be adapted by Entities

It defines 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.

This decision, approved at the Executive Committee of January 20th 2014, takes effect immediately

Jacques Perret
Group Data Privacy Officer

Alain Chaigneau
Group General Secretary

Gérard Mestrallet
Chairman & Chief Executive Officer

Document(s) cancelled or amended: xxx
Attachment(s): xxx
Distribution: xxx

GDF SUEZ HEADQUARTERS
1, place Samuel de Champlain - 92930 Paris La Défense Cedex - France
Tel. +33 (0)1 44 22 00 00
GDF SUEZ SA, CAPITAL OF € 2 412 824 089 - RCS Nanterre 542 107 651
www.gdfsuez.com

1. Background and issues

GDF SUEZ Group is required to process Personal Data relating to its employees, clients, partners, service providers, subcontractors and suppliers.

Such Personal Data are not only present in paper documents but in all of the Group's Information Systems such as company data centres, software applications, the Internet and the Intranet, the cloud, big data, smartphones, BYOD[3] (Bring Your Own Device), the smartgrid, etc.

The Group is therefore increasingly exposed to the risk of inappropriate internal / external collection and usage or of alteration, compromise and even falsification of Personal Data.

This can lead to damage of image and reputation and potentially prosecution and significant financial penalties for the Group.

Mindful of the importance of Data Privacy and the risks arising when it is breached, the Group is committed to protecting this intangible asset. Such action also has a direct positive effect on the confidence of the Group's staff and clients, as well as effect on the Group's image and reputation.

Data Privacy being a legal obligation and a strategic issue for the Group and its reputation, it is essential to implement the present policy (the "Policy").

2. Definitions

- **"Data Controller"**: the natural or legal person responsible for determining the purpose and methods of the Data Processing that have been implemented or are to be implemented. The Data Controller is bound to take every precaution necessary to ensure Data Privacy.
- **"Data Processing"**: any operation or set of operations involving Personal Data, whatever the method or means used (automated Data Processing such as IT applications, Excel data files, etc., or non-automated Data Processing included or intended to be included in a structured filing system whereby Personal Data are accessible according to specific criteria such as employees' individual paper files, etc.), particularly collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other form of circulation, alignment or consolidation, blocking, deletion or destruction.
- **"Data Processor"**: subcontractor to whom the Data Controller assigns all or part of the operations relating to its Data Processing, such as the implementation, the hosting, the operation, the management, etc.
- **"Data Protection / Privacy Officer" (DPO)**: the person designated within an Entity as responsible for actions relating to the protection of Personal Data (see chapter 5.2).

[3] Use of personal equipment (laptop computers, etc.) in a work environment.

- **“Data Privacy” / “Data Protection”** : set of **actions, activities, methods, processes,** organisations and so forth aiming at protecting Personal Data and ensuring compliance with applicable Data Privacy laws and regulations.
- **"Entity"**: legal entity within the consolidated scope of the Group (global integration).
- **"Group**": GDF SUEZ Group.
- "**Group Data Privacy Officer"**: the person appointed at Group level to define and disseminate good practices relating to Data Privacy and to ensure their application (see chapter 5.1.1).
- **"Personal Data"**: any information relating to an individual, as a natural person (‘**Data Subject’**) identified or able to be identified, directly or indirectly, by referring to an identification number or to one or more elements specific to him/her (e.g. surname, first name, social security number, email address, IP address, etc.).
- **"Project Manager"**: person acting on behalf of the Data Controller, who manages the project until the Data Processing has been implemented. The Project Manager must ensure that Data Privacy is maintained and respected throughout the project.

The glossary attached to this document contains more definitions in addition to those above.

3. Scope and objectives

The Group Data Privacy Policy is following the same values as the Group's Ethics Charter, as part of the Group’s initiative to control risks and protect its intangible assets[4]. It applies to all functional areas as specified in an Information System usage policy and to all staff and Entities of the Group, although it may be overruled by national regulations applicable to an Entity including specific regulations providing for the independence of infrastructure providers within the European Union or any other equivalent regulation applicable elsewhere.

The principles of the Group Data Privacy Policy are based on international regulations listed in Appendix 1.

The GDF SUEZ Group Data Privacy Policy defines the principles, methods and governance that will enable the Group to comply with the applicable regulations with respect to the protection of privacy in light of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights5. This Policy also anticipates certain elements of the draft European Regulation relating to

[4] See Group Tangible and Intangible Assets Security Policy (GTIASP).

[5] Article 12 of the Universal Declaration of Human Rights (United Nations): *No one shall be subjected to arbitrary interference with his privacy...*

Article 17 of the International Covenant on Civil and Political Rights (Office of the High Commissioner of Human Rights): *No one shall be subject to arbitrary or unlawful interference with his privacy ...*

Data Protection that the Group has decided to include in its basic principles as they are regarded as good practice in favour of privacy protection.
This Policy will be reinforced and made more detailed with the progressive addition of further documents (methodologies, good practices, awareness, etc.) that will enable the achievement of the objectives set.

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 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.

3.1. Lawfulness and fairness purpose

Personal Data must be collected and processed by fair means for specified, explicit and lawful purposes and must not be used or processed subsequently in a way that is incompatible with these purposes.

Compliance with these lawfulness and fairness principles may require under certain applicable Data Protection legislations:
- that the Data Subject be informed of the Data Processing and its purposes; and/or
- the Data Subject expressly consent to the Data Processing; and/or
- the local Data Protection Authority be notified of the intended Data Processing.

Personal Data may be communicated within services or departments or to other Entities of the Group or to third parties only in relation to the purposes of the Data Processing, and Data Subjects must be informed of (or sometimes shall consent to) this communication of their Personal Data.

3.2. Relevance of collected data

The Personal Data collected must be appropriate, relevant and not excessive with respect to the purposes for which it is collected and its subsequent processing. It must be accurate, comprehensive and updated if necessary.

The period of retention of the processed Personal Data must be defined in accordance with the purpose of the collection and with regard to applicable laws. Once Personal Data are no longer needed for the purpose legitimizing their processing, they must be deleted or rendered anonymous.

3.3. Sensitive Data

Some Personal Data are deemed to be sensitive. These Data involve the Data Subjects' most intimate sphere or are likely to give rise, in case of misuse, to unlawful or arbitrary discrimination.

In particular, Personal Data providing for racial or ethnic origin, political, religious or philosophical opinions or beliefs or relating to a person's health or sex life, are to be considered sensitive.

In addition, it is necessary to verify the Data Privacy laws applicable to the Entity, to identify any other Personal Data deemed sensitive and to comply with specific requirements relating to sensitive data pursuant to applicable laws.

A Data Controller should not process Sensitive Data unless explicit consent is given by the Data Subject or under limited circumstances specifically allowed by the law.

3.4. Confidentiality and Security obligations

All appropriate protection measures must be taken with regard to the nature of the data and the risks presented by the Data Processing to ensure that Personal Data are secure and kept confidential and, in particular, to protect them from being distorted or damaged and prohibit unauthorized access.

These measures will depend on the existing risk, the possible consequences on the Data Subject, the sensitive nature of the Personal Data, the available technology and the general accepted practice in the jurisdictions relevant to the Entity.

Data Processors will be selected for their ability to offer guarantees in respect of the technical and organizational security and confidentiality measures of their processing. A contract must be established providing for the Data Processor's obligations to comply with these safeguards.

3.4.1. Classification and Protection of Personal Data

Personal Data are classified as "Internal" or "Restricted" (according to the Group Tangible and Intangible Assets Security Policy/Rule Group 11).

Sensitive Data are classified as "Restricted" or "Confidential" (see Rule Group 11).

The classification of Personal Data should be identified at the stage of Privacy impact assessment (see 3.4.2 *Upstream risk process*).

Personal Data must be protected in accordance with GDF SUEZ policies and security standards relating to the Information Systems.

3.4.2. Upstream risk process

The implementation of new Data Processing activities must be accompanied by the following actions throughout the different phases of the project:

- Privacy impact assessment: this determines the level of risk for the Data Subjects (i.e. in the event of loss or compromise of their Data) and for the Entity (i.e. in the event of harm to its image or its reputation) and aims at identifying adequate protection measures.

- Privacy by design: this implies that the technology system and solutions incorporate Data Protection and Privacy at the earliest stage possible of its design and development.

- Privacy by default: this involves the settings of Data minimisation (those strictly necessary for the purposes of the Data Processing), Data retention (specifically related to the purposes of the Data Processing) and de-identification (anonymisation).

It is important to take all necessary measures to ensure protection of Personal Data at all phases of the project.

3.5. International transfers

As a general rule, international transfers of Personal Data may be carried out when the country to which such data are transmitted offers, as a minimum, the level of protection described in this policy.

Appropriate contractual clauses shall otherwise be included in agreements concluded between the senders (the “Exporters”) and the recipients (the “Importers”) of Personal Data, in order to guarantee an adequate level of protection of such Data.

Besides, GDF SUEZ has set up BCR (Binding Corporate Rules), approved by the European Data Protection Authorities, in order to ensure the protection of Personal Data transferred outside of the European Union, within the Group. Such internal rules are embedding legal data privacy obligations and shall be known and complied with by all employees of the Group.

3.6. Openness and respect for individuals' rights

Data Subjects have the right to control the information relating to their person. They shall be informed of any Data Processing of their Personal Data prior to the effective implementation of the Data Processing and they benefit at any time of a right of access to and rectification of their Personal Data. Data Subjects also have the right to object at any time to the processing of their Personal Data based on compelling legitimate grounds relating to their specific personal situation, even if they had given their express consent to this processing.

Transparent policies shall be implemented with regard to Data Processing. Therefore, basic information shall be provided to Data Subjects with respect of Data Controllers’ identity and the way Data Subjects may exercise their rights to access, rectify and/or require deletion of their Personal Data.

4. Means

The following actions will be implemented in order to achieve the objectives of this Policy:

4.1. Awareness and training

All personnel must be made aware of the issues involving Data Privacy. Global awareness campaigns will be conducted at Group level. Local actions may be carried out by the Entities to complement these campaigns.

Training of Data Protection Officers will be conducted according to the same principles.

These actions must be coordinated within the Entities by the Group Data Privacy Officer and the DPOs.

4.2. Reviews and Audits

Internal reviews for compliance with the present Policy and the Data Protection laws must be carried out regularly by the Entity's Legal Representative who will delegate this activity to its DPO and IS Security Officer. The Group Data Privacy Officer may also proceed with such reviews.

As part of these reviews, access to processes and Data, as well as the confidentiality and security measures and retention periods are to be assessed and controlled.

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

4.3. Data Process mapping

In relation with the Openness principle and to facilitate the exercise of the Data Subjects' right of access, it is recommended that each Entity establishes a map and a register of all Data Processing. As well as offering a comprehensive overview, this map will allow for the Data Processing to be controlled and rationalized and the register will facilitate the Data Controller’s handling of the Data Subject’s access request.

4.4. Incident Handling

Any person being aware of an inappropriate use of Personal Data will contact his DPO who will address this incident to his Ethics Officer, the latter being in charge of reporting this incident to INFORM’ethics.

As soon as it is clear that an incident has a potential impact on Data Privacy, the Group Data Privacy Officer should be informed and will handle the issue in liaison with the other members of the Incident Handling Committee (along with the Entity concerned).

In the event that crisis management is required to handle the incident, the Group Data Privacy Officer shall be one of the designated members of the crisis centre for the resolution of the incident.

Security incidents must be handled in accordance with the Security Incident Management Procedure[6].

4.5. Written agreements

In the cases of acquisition, use or sub-contracting of Personal Data (for example, for the provision of additional offerings to GDF SUEZ's clients and prospective clients) a written agreement must be established between the parties concerned (GDF SUEZ, its clients or partners). Under all circumstances, the collection, use or subcontracting of Personal Data must comply with the laws in force, the GDF SUEZ Ethics Charter and the present Policy.

5. Governance

The principles and methods described above shall be implemented at Group level and within each Entity.

5.1. At Group level

The strategic management of this Group Data Privacy Policy is the responsibility of the GDF SUEZ General Management Committee, which delegates the coordination and operational management of the Policy to its Group General Secretary. The Group General Secretary delegates this responsibility to the Group Data Privacy Officer.

Any difficulty in applying this policy must be escalated to the Group Data Privacy Officer.

5.1.1. Group Data Privacy Officer

The principal responsibilities of the Group Data Privacy Officer are as follows:

- To define and disseminate, in collaboration with the Entities, good practice relating to the use and processing of Personal Data (clients, suppliers, employees etc.).
- To ensure the correct application of the Group Data Privacy Policy and to advise/alert managers about the associated risks.
- To encourage the creation of value in the use of Personal Data by promoting synergies amongst the various Data Processing activities for which different Entities are responsible.
- To establish a group wide network of individuals responsible for Data Protection.
- To represent the Group in this area with external stakeholders and organizations.
- To monitor the development of regulation in the main countries where the Group is based.
- To coordinate the management of incidents relating to Data Privacy with Sponsor Divisions of INFORM'ethics.

[6] Procedure approved by the Information Security Committee in October 2012 then by the Executive Committee (COMEX).

5.1.2. The Data Privacy Committee

The Data Privacy Committee (DPC) is constituted by this Policy and shall manage all activities relating to Data Privacy.

The DPC is chaired by the Group Data Privacy Officer and meets every quarter, attended by the Data Protection Officers appointed at Business Line level. The DPC also includes a representative from the Legal Division, the Ethics Division, the Internal Audit Division and the Human Resources Division of the Group as well as, if required, the Group IS Security Officer, a representative from the Health and Safety Department and the Security Director acting as representative of the Information Security Committee of the Group.

It decides local or transversal actions at its level and submits them to Group-level bodies, and if applicable to the GDF SUEZ General Management Committee, for approval.

Once a year, the DPC shall carry out a review of its activities (including an update on the application of this Policy) and shall present it to the Group-level bodies concerned.

Once a year, the DPC shall organize an internal workshop with the objective of bringing together representatives of all stakeholders concerned by Data Privacy. This event shall be a forum for discussion and sharing for all those involved. It shall also be an opportunity to present the review of the previous year and the strategic directions for the year to come.

5.2. At Business Line and Business Unit level

Each Business Line shall appoint a Data Protection Officer (DPO) who coordinates the activities relating to Data Protection within their area of responsibility.

The missions of the DPO are the following :

- To implement the Group Data Privacy Policy and control its application.
- To inform, advise and if necessary alert Data Controllers about Data Protection issues.
- To be involved in the awareness campaign among staff.
- To participate in the activities organized by the Group Data Privacy Officer (good practices, feedback from past experience, etc.) and to be an active member of the network.
- To prepare an annual report of its activities
- To report any incident in collaboration with the Ethics Officer (cf. 4.4).

Where appropriate, a Business Line may also decide to identify DPO at Business Unit levels.

Data Protection could also be organized at country level when efficiency may require this approach.

5.3. At Entity level

Each Entity is responsible and accountable for the Data Processing that it implements (or that it has implemented by a Data Processor) and the Legal Representative of the Entity shall be responsible for ensuring compliance with the Data Protection laws applicable to that Entity.

Each Entity shall ensure compliance with the Group Data Privacy Policy and Data Protection laws before the implementation of Data Processing and throughout its execution and operation.

When required by law, the DPO (or a person specifically appointed) shall be in charge of compliance with local laws requiring, for instance, that Data Processing activities are notified to the relevant national Data Protection Authority.

5.4. Other stakeholders

The IS Security Officers shall offer its expertise and support in the area of Data Privacy, both for the purposes of data processes hosted internally and with a third party. The IS Security Officer's primary functions in this area are as follows:

- To assist DPOs in the classification of Personal Data (see Rule Group 11) and in the roll out of the IS project management (see*3.4.2 Upstream risk process)*.
- To advise on the selection of Data Privacy functions and systems.
- To be the contact point for all requests relating to the technical aspects of Data Privacy for a Data Processing in production.

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.

The Legal and Human Resources Divisions shall offer advice and information with respect to the applicable legislation and jurisprudence.

The Ethics Officers shall give advice to the respective DPO in relation with INFORM'ethics.

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

All personnel implementing an application that processes Personal Data must first inform the DPO of the Entity, as Data Processing may require prior notification to a Data Protection Authority.

Any third party 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.

Appendix 3: Data Processing

Scope : Categories of Data and Purposes of Data Transfers and Processing covered by the BCR

The BCR apply to all the Human Resources Personal Data of the Group that is or has been subject to the EU Directive, and more specifically to all Personal Data of the Group's employees, candidates, trainees, temporary workers, or retirees, that are collected in the EEA, transferred and processed within the Group to manage its human resources at international levels as part of its business, i.e. :

- Organization (directories, organizational charts, as well as controlling access to the Group's IT Systems for traceability or system monitoring purposes, …),
- Compensation and benefits (annual increases, flexible pay, gross salary, share holding, …),
- Recruitment and national / international mobility,
- Human resources development (skills, training, performance assessment, development plans, …) ,
- Staff administrative management (personal data management, payroll, time management, travel allowance/expenses, …),
- Whistle blowing (ethics events, discrimination, …),
- Health, safety and environment (travel safety, personal accidents, …)
- Security incident management (forensics, …),

Appendix 4: GDF SUEZ Information System Security

Group and Thematic Security Policies

- Group IS Security Policy: Describes the whole organization of the security network of the Group, the various committees as well as the roles and the responsibilities of each of the players.
- Thematic Policy on Passwords Security : Describes the constraints bound to the construction and the management of the passwords for the whole IS.
- Thematic Security Policy on IAM (Identity Access Management) : Describes the security constraints applicable to the management of the identities and the user accounts, the access rights and the authorizations.
- Thematic Security Policy for Networks and Telecom: Describes all the security constraints bound to the network and the telecoms resources of the Group, in particular the datacenter's security.
- Thematic Security Policy on Internet Access: Describes all the security constraints applicable to the implementation and the use of the internet access of the Group in particular the necessity of setting in place a filtering policy of the accessible sites by the users
- Thematic Security Policy on Partner Access: Describes all the security constraints applicable to the accesses of the external partners on our IS whatever the access type: permanent, temporary, remote …
- Thematic Security Policy for Remote Access: Describes all the security constraints bound to the accesses in our IS from the outside for the employees of the Group, in particular as regards the accessible resources, the necessity level of authentication, etc. …
- Thematic Security Policy on Hosting Service Requirements: Describes all the security constraints applicable to the external hosting of internal resources of our IS that have to be respected by the hosting service.
- Thematic Security Policy for Internet and Extranet Web Sites Hosted by a third party: Describes all the security constraints bound to the external hosting of web sites / Extranet of the Group that have to be respected by the hosting provider.
- Thematic Security Policy for Internet Points-of-Presence: Describes all the security constraints applicable to the Group's points of presence on the Internet: Web sites, routers of interconnection …
- Thematic Security Policy for Application Acceptance Tests: Describes all the security constraints bound to the test of the Web applications developed by the Group (tests of security to be done before going live).
- Thematic Security Policy on Wi-Fi: Describes all the security constraints applicable to the use of the WIFI technologies within the Group, whether it is to reach the local LAN of an entity or to give Guest's access to the visitors.

- Thematic Security Policy for Vulnerability and Patch Management: Describes the process to be set up within every entity for the management of the vulnerabilities and the security patch according to their criticality.
- Thematic Security Policy on Workstations and Mobile Device Security: Describes all the security constraints bound to the use of the user workstations and the mobile devices, in particular in terms of encryption, antiviral protection …
- Thematic Security Policy for Datacenter Virtualization: Describes all the security constraints applicable to the use of the technologies of virtualization within IS: protection of the virtual images, the physical servers, the exploitation, the supervision …
- Thematic Security Policy for Active Directories : Describes all the security constraints bound to Active Directories: exploitation, supervision, account reviews, the access rights management…
- Thematic Security Policy for Contingency Planning : Describes all the security constraints to be respected to insure the continuity of IT activity within an entity and its maintaining in operational conditions.
- IS Protection Plan: Describes all the security constraints bound to the life cycle of the information, according to its confidentiality level (access, protection, transport, deletion)

Other documents related to Information Security :

- Protection policy of tangible and intangible assets: Describes the whole protective framework which protects the sensitive information at its appropriate level, gives responsibilities to all the players and guarantees an adaptation to the threats.
- Group Rule n°11 on the classification of the information, defines 4 confidentiality levels for information and identifies the security constraints to apply accordingly.

Appendix 5: Personal Data Protection Clause

1.1. In order to perform the Framework Agreement and/or the Implementation Agreement Service Provider has to process data concerning customers and employees of Customer, and among others, personal data. Such personal data are particularly sensitive for the corporate image and capital of Customer.

1.2. Each Party is informed that personal data and their related processing are subject to legal provisions and regulations referred to as the French law on data-processing and liberties (and notably the law of 6 January 1978). If required, each Party shall process during the term of the Framework Agreement to any declaration or statement and more generally shall comply with the regulation on data-processing and liberties.

1.3. Customer remain the owner of all the data processed by Service Provider under the Framework Agreement.

1.4. Service Provider undertakes to comply with all the directives, guidelines and recommendations formulated by Customer in this respect.

1.5. Service Provider undertakes, under the Framework Agreement and/or Implementation Agreement to take the safety measures in order to:

- Ensure the safety and integrity of personal data against any disclosure, bribery, destruction, hacking of such data by a non-authorised third party;
- Not use the personal data for an aim other than for the strict performance of its contractual obligations. Therefore, Service Provider shall refrain from processing, including for its own needs, directly or indirectly, such data. Service Provider commits not to sell or give or make at the disposal the data and files for any purpose and, among others, commercial purposes;
- Not keep such personal data more than the time required for the performance of its contractual obligations;
- Ensure safety, integrity and confidentiality;
- Take all required steps in order not to spread a virus;
- Not forward data collected toward a country which does not have sufficient protection, in the sense of the European Directive on Data Protection, without prior written agreement of Customer;
- Use of the appropriate contractual clauses proposed by the European Commission signed by entities located in such a country in all cases of transfers of personal data

to a country that does not have adequate protection within the meaning of the DIRECTIVE 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

- Not take copies of any documents and information media containing personal data, except for those required to perform the Services and process or make process among sub-contractors, at the end of the Agreement, at the destruction of data, computerized or paper files containing data collected under the Agreement;

- Ensure that any data breach is reported to the Customer within 48 hours of its detection, and take appropriate measures in order to mitigate the consequences of such data breach.

1.6. Customer reserves the right to process or to make process any reasonable checkout that would appear essential to ascertain the compliance with the aforesaid obligations of Service Provider, after having informed the latter.