SUMMARIZED VERSION
OF TOTAL'S BINDING CORPORATE RULES

1. Introduction

The Total Group (or "Total") promotes a culture and practices regarding the protection of personal data[1], in accordance with the applicable laws. To this end, Total has implemented Binding Corporate Rules ("BCRs").

This document summarizes the data protection principles that apply under our BCRs and the rights granted by them.

2. Purpose

Our BCRs are a set of internal binding rules, which are applicable to all of the Total subsidiaries that have adopted them. They have been approved by the European data protection authorities.

They allow Total subsidiaries to transfer personal data originating from the European economic area ("EEA")[2] to Total subsidiaries located outside of the EEA in compliance with the applicable law.

3. Implementation scope

Our BCRs apply to all EEA-originating personal data processed by Total subsidiaries including data relating to former and current employees, job applicants, clients and prospective clients, suppliers and sub-contractors and the staff of third companies acting on behalf of the Group subsidiaries as well as shareholders (hereafter "data subjects").

4. Protection principles

The following principles set out in our BCRs must be respected, among which:

- **Lawfulness**

Any processing[3] operation carried out has a legal basis, provided by the applicable law.

Personal data must only be processed for lawful, determined and legitimate purposes. The data must not be further processed in a way which is incompatible with those purposes.

- **Relevance**

Personal data must be accurate and proportionate, in terms of quality and quantity, in relation to the purpose of the processing.

- **Transparency**

Personal data must be obtained lawfully and loyally. Data subjects must be informed about the characteristics of the processing of their personal data and about their rights, unless this proves impossible or would involve disproportionate efforts.

---

1 *Personal data means any information enabling the direct or indirect identification of a natural person.*

2 *EEA means Member States of the European Union plus Iceland, Liechtenstein and Norway.*

3 *Processing means any operation which is performed upon personal data, whether or not by automatic means (e.g: collection, recording, storage, destruction…).*

- **Security**

Personal data must be protected by appropriate security measures to limit the risks of unauthorized access, destruction, alteration or loss.

To do so, a set of internal norms apply, allowing to ensure the security and the confidentiality of personal data:

- The usage Charter for the IT and communication resources, that requires to act in accordance with the regulation and with the confidentiality rules;
- The Information Systems Security policy, that defines the governance mode of the security of information systems;
- The Information Systems Security Reference System, that enumerates, through 19 detailed themes, the different requirements of the Group in terms of security of information systems;
- The Information Protection policy, that presents the requirements relative to the protection of confidentiality, integrity and of the availability of the information held and exchanged within the Group

When calling upon the services of a third party to process personal data, Total subsidiary makes sure that the latter offers sufficient guarantees as regards the security and confidentiality of data.

- **Retention**

Personal data must be retained only for a reasonable and not excessive period of time with regard to the purpose of the processing.

When the retention period expires, the data is destroyed, anonymized or archived.

- **International transfers[4] of personal data**

Total does not transfer personal data originating from a country of the EEA directly to a Total subsidiary located in a third country which does not provide an adequate level of protection, unless such subsidiary has formally subscribed to the BCRs or uses another legal instrument recognized by the European Commission.

Total does not transfer personal data originating from the EEA directly to a company not belonging to the Group located in a country which does not provide an adequate level of data protection (data controller or processor) without a legal basis under applicable law and instruments providing for sufficient safeguards, such as the standard contractual clauses.

Similarly, where a data importer further transfers personal data originating from the EEA to a company not belonging to the Group (data controller or processor) located in a country which does not provide an adequate level of data protection, the data importer shall enter into an agreement with this company whereby it commits to observe the principles of BCRs.

5. Data subject rights

Under our BCRs, data subjects whose personal data are processed have the following rights:

- Right of access to the data

- Right to rectify, erase and lock data

4 *Transfer means all virtual and physical exchanges of EEA-originating personal data from one country to another.*

- Right to object to the processing

- Right to limit the processing

[A comprehensive list of the rights granted by the BCRs is detailed in APPENDIX 1 hereafter].

Data subjects may exercise these rights by submitting a request using the contact details provided in the legal notice concerning the processing of their data. Total subsidiaries undertake to give replies within the legal deadline about queries concerning the processing outside the EEA.

Moreover, if data subjects believe that a Total subsidiary has failed to observe the BCRs, they have the right to lodge a complaint by sending:

- An e-mail to: data-protection@total.com

  or

- A letter to TOTAL – DATA PROTECTION, Tour Coupole, 2 place Jean Millier, Arche Nord Coupole/Regnault, 92078 PARIS LA DEFENSE CEDEX.

Data subjects will be informed about the status of their complaint and of any further steps.

The internal complaint procedure is described in APPENDIX 2 hereafter.

The fact that data subjects may file a complaint with Total does not affect their rights to lodge a complaint with the competent EEA data protection authorities or to bring an action before the courts of the EEA country where the Total subsidiary responsible for exporting the personal data is established.

6. Governance

An internal « personal data Protection network » is in charge of monitoring and controlling the implementation of the BCRs within the Group. It is composed of:

- A Corporate Data Privacy Lead who monitors and follows compliance actions at the Group level;
- Branch Data Privacy Leads who lead and coordinate compliance actions at the Branch level;
- Data Privacy Liaisons who lead and coordinate compliance actions at the affiliate level.

7. Internal control and audit

To ensure the proper application of our BCRs, some internal control and audit mechanisms have been implemented.

An annual internal control plan is defined by the personal data Protection network to assess the level of compliance of the Group's processing regarding our BCRs. A reporting is also set up to report regularly on the actions plans that have been drawn up after evaluations.

Furthermore, the Group Internal Audit Direction also integrates the control of the personal data protection pattern into its periodic audit plan.

8. Changes to Total's rules

If necessary, our BCRs may be completed or updated.

9. More information

A copy of the comprehensive version of our BCRs as well as a list of Total subsidiaries that adopted them can be obtained by sending an e-mail at: data-protection@total.com

APPENDIX 1
THIRD PARTY BENEFICIARY RIGHTS

Our BCRs grant rights to Data Subjects to enforce the Rules as third-party beneficiaries.

More specifically, they may enforce the following principles according to the terms and conditions set out in our BCRs:

- That any processing operation carried out within the Group must have a legal basis as provided for by Applicable Law;

- That Total must collect and process Personal Data for legitimate, specified and explicit purposes and must not further process any Personal Data in a way incompatible with the purpose for which they were collected;

- That Total must process Personal Data that are relevant and not excessive in relation to the purposes for which they are collected, and that these Data must be accurate and, where necessary, kept up to date;

- That Data Subjects must be provided with easy and permanent access to the information relating to their rights under these BCRs;

- That Data Subjects whose Personal Data originate from the EEA must have a right of access, of rectification and of objection to the processing of their Personal Data in accordance with Applicable Law;

- That Data Subjects whose Personal Data originate from the EEA must not be subject to a decision that produces legal effects concerning them or significantly affects them and that is based solely on automated processing of Personal Data intended to evaluate certain personal aspects relating to them, unless that decision:

    - Is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the Data Subject, has been satisfied or that there are suitable measures to safeguard his/her legitimate interests, such as arrangements allowing him/her to express his/her point of view; or

    - Is authorized by Applicable Law, which also lays down measures to safeguard the Data Subject's legitimate interests;

- That Total must implement appropriate measures to guarantee the security and confidentiality of the Personal Data, having regard to the state of art and the cost of their implementation;

- That Total must conclude a written processing agreement with any service provider used to process Personal Data, specifying that the service provider shall act only under Total's instructions and shall implement appropriate security and confidentiality measures;

- That Total must not transfer Personal Data from a Member State of the EEA or originating from the EEA to a company not belonging to the Group and located in a Third Country which does not provide an adequate level of data protection (either an External Data Controller or Processor) without a legal basis under Applicable Law and instruments providing for sufficient safeguards;

- That a Total Subsidiary must immediately inform the Data exporter if this Total Subsidiary deems that the legislation applicable in its jurisdiction is likely to prevent it from fulfilling its obligations pursuant to Total's BCRs, and have a detrimental effect on the guarantees offered by these BCRs, unless where prohibited by a law enforcement authority, in particular as a result of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

- That any Data Subject may lodge a complaint with Total through the internal complaint mechanism in accordance with the terms set out in the Chapter « Complaint handling »;

- That any Total Subsidiaries that have subscribed to the BCRs must cooperate with the competent supervisory authorities, follow their recommendations regarding the international Transfers of Data in the event of a complaint or of a particular request from such authorities and accept to be audited by the supervisory authority of their country of establishment;

- That any Data Subject may lodge a complaint with the National Supervisory Authorities or bring an action before the court of the EEA Member State where the Data exporter is established in order to enforce the above principles, and, where appropriate, to receive compensation for the damage suffered as a result of a breach of Total's BCRs. If, in the course of a transfer of Personal Data outside the EEA, the Data importer fails to observe Total's BCRs, the Data exporter will defend any claim, establish that the Data importer has not violated the BCRs, and pay compensation to the Data Subject for the damage suffered as a result of that violation.

APPENDIX 2

INTERNAL COMPLAINT HANDLING PROCEDURE

If a Data Subject believes that a Total Subsidiary has not complied with Total's BCRs, he/she may file a complaint in accordance with the complaint procedure set forth in the relevant privacy policy or contract or pursuant to the procedure described below.

1) How to make a complaint

Data Subjects may file a complaint by sending:

- An e-mail to: data-protection@total.com

  or

- A letter to TOTAL – DATA PROTECTION, Tour Coupole, 2 place Jean Millier, Arche Nord Coupole/Regnault, 92078 PARIS LA DEFENSE CEDEX.

The complaint should clearly provide as much detail as possible about the issue raised, including:

- The country and the Total Subsidiary concerned, the Data Subject's understanding of the violation of the BCRs, the redress requested;

- The Data Subject's full name and contact details as well as a copy of his/her identity card or any other identifying document;

- Any previous correspondence on this specific issue.

2) Total's response

Within three months of Total receiving a complaint, the appropriate Branch Data Privacy Lead ("BDPL") shall inform the Data Subject in writing of the admissibility of the complaint; and if the latter is admissible, of the corrective actions that Total has taken or will take in response. The appropriate BDPL shall ensure that, if necessary, appropriate corrective actions are taken to achieve compliance with the BCRs.

The appropriate BDPL shall send a copy of the complaint and any written reply to the Corporate Data Privacy Lead ("CDPL").

3) Recourse process

If the Data Subject is not satisfied with the response from the appropriate BDPL (e.g., the complaint has been rejected), he/she may refer to the CDPL by sending an e-mail or letter as indicated above. The CDPL will review the complaint and reach a decision within three months of the data the request was received. Following this period, the CDPL will inform the Data Subject whether the initial response has been upheld or communicate a new response.

The fact that Data Subjects may file a complaint with Total does not affect their right to lodge a complaint with the competent National Supervisory Authority or bring an action before the court of the EEA Member State where the Data exporter is established.