# ANNEX 1

## *« BINDING CORPORATE RULES »*

V-2017

---

### FOREWORD

The TOTAL Group (hereinafter « TOTAL » or « the Group ») values the individual rights and freedoms and processes Personal Data in compliance with the applicable laws and regulations.

In order to ensure an adequate level of protection of the Personal Data being transferred outside the European Economic Area (hereinafter « EEA »), TOTAL implements these internal Rules relating to the Transfer of Personal Data (hereinafter « Binding Corporate Rules » or « BCRs »), which are applicable to all of the TOTAL Subsidiaries that subscribe to them.

These BCRs have been drafted so as to meet the requirements of the European legislation applicable to the protection of Personal Data. The TOTAL Subsidiaries concerned thereby display their commitment to adopt common rules legally governing their intercompany Transfers of Personal Data originating from the EEA.

It is every Employee's duty to know TOTAL's BCRs and to observe its principles in the context of his or her activities within the Group.

The TOTAL Subsidiaries, which intend to benefit from the legal regime offered by the BCRs, must adopt them in compliance with their respective decision-making rules and with applicable law in the jurisdiction where the TOTAL Subsidiary concerned is established ; and must commit, by means of an Intra-Group agreement, to receiving and transferring Personal Data originating from the EEA across the world in compliance with the BCRs.

<u>Structure of the Binding Corporate Rules</u>

- Implementation scope ;
- Protection principles ;
- Governance ;
- Training program ;
- Security ;
- Impact assessment ;
- Complaint handling ;
- Internal control and audit.

The rights granted to Data Subjects as third-party beneficiaries in these various chapters are summarized in APPENDIX 1 to the BCRs.

The TOTAL Subsidiaries that subscribe to these BCRs by signing an Intra-Group agreement commit to complying with all the principles and conditions as detailed in these chapters.

These BCRs may be completed or updated, as need be, according to the terms and conditions set out in the chapter « Governance ».

# SUMMARY

## GLOSSARY

- **APPLICABLE LAW**
  Any European and national legislation in force governing the protection of Personal Data in the Member States of the European Economic Area.

- **BINDING CORPORATE RULES (« BCR »)**
  Binding Corporate Rules relating to the transfers of Personal Data outside the European Economic Area that are applicable within the TOTAL Group.

- **BRANCH DATA PRIVACY LEAD (« BDPL »)**
  The individual(s) responsible within their Branch for implementing and properly applying TOTAL's BCRs.

- **DATA** or **PERSONAL DATA**
  Any information relating to an identified or identifiable natural person ; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

- **DATA CONTROLLER**
  Any TOTAL Subsidiary that determines the purposes and means of the Processing of Personal Data.

- **DATA EXPORTER**
  Any Data Controller established in the European Economic Area that transfers Personal Data to a Data Importer in a Third Country or on whose behalf another TOTAL Subsidiary in the European Economic Area transfers Personal Data to a Data Importer in a Third Country.

- **DATA IMPORTER**
  Any TOTAL Subsidiary established in a Third Country that is receiving Personal Data originating from the European Economic Area for further Processing.

- **DATA RECIPIENT**
  Any physical or legal person, public authority, or any department or entity having access to Personal Data or to whom Personal Data are disclosed.

- **DATA SUBJECT**
  Any physical person whose Personal Data undergoes Processing in his capacity as an Employee, a job applicant, an employee of a third company acting on behalf of TOTAL, a client or prospective client, or a supplier of the TOTAL Group.

- **EMPLOYEE**
  Any individual working directly for TOTAL S.A. or one of the TOTAL Subsidiaries.

- **EUROPEAN ECONOMIC AREA (« EEA »)**
  Member States of the European Union plus Iceland, Liechtenstein and Norway.

- **EXTERNAL DATA CONTROLLER**
  Any company that is not a TOTAL Subsidiary and determines the purposes and means of the Processing of Personal Data.

- **CORPORATE DATA PRIVACY LEAD (« CDPL »)**
  The individual responsible at the headquarters of the Group for managing and coordinating activities for implementing and properly applying TOTAL's BCRs.

- **NATIONAL SUPERVISORY AUTHORITY** or **SUPERVISORY AUTHORITY**
  Administrative authority of a Member State of the European Economic Area which is responsible for monitoring the application in its territory of the applicable legal and regulatory provisions relating to the protection of Personal Data.

- **POLICY**
  Any TOTAL corporate document setting out the fundamental principles relating to a specific topic, and providing a framework from which the content and conduct of the policies relating to these topics will be adapted in the TOTAL Subsidiaries.

- **PROCESSING**
  Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

- **SENSITIVE DATA**
  Any Personal Data that reveals, directly or indirectly, the racial or ethnic origin, political or philosophical opinions, religious beliefs, trade union membership, physical or mental health or sex life or the criminal record of an individual.

- **PROCESSOR**
  Any internal or external company which processes Personal Data on behalf of, and on the instructions of, a TOTAL Subsidiary.

- **THIRD COUNTRY**
  Any country that is not a Member State of the European Economic Area.

- **TOTAL or GROUP or TOTAL GROUP**
  All TOTAL Subsidiaries.

- **TOTAL SUBSIDIARY** or **SUBSIDIARY**
  TOTAL S.A. or any company of which over 50% of the voting rights are or would be held directly or indirectly by TOTAL S.A.

- **TRANSFER**
  Any operation or set of operations which support the communication, copy or movement of Personal Data by using a network or any other medium, to the extent that those Data are intended to be processed by the Data Importer.

# IMPLEMENTATION SCOPE

## I. MATERIAL SCOPE

TOTAL's BCRs apply to all Processing operations, Transfers and Data Subjects described hereunder. These BCRs may apply to future activities, in which case the material scope will be updated, if necessary.

- **Data Subjects**

TOTAL's BCRs apply to Personal Data about :

- Job applicants ;
- Employees ;
- The staff of third companies acting on behalf of the TOTAL Subsidiaries that have adopted these BCRs ;
- Clients and prospective clients ;
- Sub-contractors and suppliers of TOTAL ;
- TOTAL's shareholders.

- **Purposes of the Processing / Transfer**

Personal Data relating to job applicants and Employees are processed for the purposes of the administrative management of the Data Subjects, and to manage the material and immaterial resources allocated to them for the purpose of carrying out their duties within the TOTAL Group, in particular :

- Recruiting ;
- Payroll ;
- Human resource management, in particular Employees' training, career development, Employees' evaluations and mobility management ;
- Administration of retirement and social security schemes ;
- Management of access control and access to the company restaurant ;
- Management of IT and communication resources (including internal identifiers) ;
- Management of business assets (including leasing vehicles) ;
- Occupational medicine ;
- Social and cultural activities (except when managed by the Works council) ;
- Internal and external communication ;
- Management of crises and of business continuity schemes ;
- Logistics and management of geolocation data.

Personal Data relating to clients and prospective clients, sub-contractors and suppliers of TOTAL and the staff of third companies acting on behalf of the TOTAL Subsidiaries that have adopted these BCRs are processed for the purposes of managing the relationships with these parties, in particular :

- Management of contracts and related operations with clients, prospective clients and suppliers ;
- Internal and external communication ;
- Management of TOTAL payment cards ;
- Accounting ;
- Logistics ;
- Management of geolocation data ;
- Management of research and strategy development and HSEQ initiatives (Hygiene, Security, Environment, Quality).

Personal Data relating to TOTAL's shareholders are processed for the purposes of managing the relationships with shareholders, in particular :

- Organization of shareholders' meetings and votes ;
- Payment of dividends ;
- Internal and external communication.

- **Nature of processed Data**

For the above-mentioned purposes, TOTAL collects and processes in particular the following categories of Data :

- Professional and private identification data (including the internal identifier, address, telephone number and e-mail address) ;
- Data related to Data Subjects' personal lives ;
- Data related to data Subjects' professional lives (including job applications, education and professional experience) ;
- Economic and financial information ;
- Traffic data ;
- Images ;
- Health-related data ;
- Geolocation data.

## II. GEOGRAPHICAL SCOPE

TOTAL's BCRs are meant to cover all Transfers of Personal Data originating from the EEA to TOTAL Subsidiaries outside the EEA that may receive, access or process Personal Data in the course of their business activities.

## III. TEMPORAL SCOPE

TOTAL's BCRs are meant to cover all Transfers of Personal Data originating from the EEA to TOTAL Subsidiaries outside the EEA that may receive, access or process Personal Data in the course of their business activities.

TOTAL will not transfer any Personal Data originating from the EEA to a new TOTAL Subsidiary outside the EEA until such Subsidiary is effectively bound by the BCRs and can deliver compliance or the Transfer relies on another legal instrument recognized by the European Commission as providing an adequate level of protection, such as the standard contractual clauses adopted by the European Commission for the Transfer of Personal Data to Third Countries (hereinafter « Standard Contractual Clauses »).

## IV. RELATIONSHIP BETWEEN NATIONAL LEGISLATION AND TOTAL'S RULES

If a Group 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 offered guarantees,

Such Subsidiary shall immediately inform the Data Exporter, 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.

Where there is conflict between national law and the commitments in TOTAL's BCRs, the Data Exporter will take a decision on what action to take and will consult the competent National Supervisory Authorities in the case of any doubts.

If, in a specific country, TOTAL's BCRs offer a level of data protection below the level required by the national legislation, the latter shall prevail over the BCRs.

## PROTECTION PRINCIPLES

The principles laid down hereunder are cumulative.

### I. ANY PROCESSING OPERATION MUST BE LEGITIMATE AND LAWFUL

Any Processing operation carried out within the TOTAL Group has a legal basis. In most cases, the Data Processing is necessary for the performance of a contract between a TOTAL Subsidiary and a Data Subject consistent with a corporate purpose. In all other cases, the Processing is based on one of the legal bases provided for by Applicable Law.

TOTAL collects and processes Personal Data for legitimate, specified and explicit purposes, and does not further process any Data in a way incompatible with the purpose for which they were collected.

### II. THE DATA MUST BE RELEVANT IN RELATION TO THE PURPOSES OF THE PROCESSING

TOTAL only processes Personal Data that are relevant and not excessive in relation to the purposes for which they are collected. In particular, the nature and the quantity of the collected Data are not disproportionate in relation to the purpose of the Processing. In addition, the Data are accurate and, where necessary, kept up to date.

TOTAL does not collect Sensitive Data, except in specific and limited cases. In such cases, the Sensitive Data are processed in compliance with Applicable Law and rely on one of the following legal bases :

- The Data Subject has given his/her explicit and prior consent ;
- The Data Subject has voluntarily made public the Sensitive Data pertaining to him/her ;
- TOTAL must fulfil a legal obligation in the field of employment law ;
- It is necessary to protect the vital interests of the Data Subject, when the Data Subject is physically or legally incapable of expressing consent ;
- It is necessary for the establishment, exercise or defence of a legal claim ;
- It is required for medical purposes (for instance for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, the management of health-care services) and those Data are processed exclusively by a health professional subject to the obligation of professional secrecy ;
- The Data are processed by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim in the course of its legitimate activities with appropriate guarantees.

### III. THE DATA MUST BE RETAINED FOR AN ADEQUATE PERIOD OF TIME

TOTAL retains Personal Data for the period necessary for the achievement of the purpose for which they were collected.

For each Processing operation, TOTAL establishes a retention period appropriate to the purpose of the Processing or to the applicable legal or regulatory provisions, in accordance with its Document Retention Policy.

After expiration of the retention period, the Personal Data are erased, anonymized or archived in accordance with the applicable statute of limitation requirements.

## IV. THE DATA SUBJECTS MUST BE INFORMED PRIOR TO ANY PROCESSING

The Data Subjects are provided with easy and permanent access to the information relating to the principles and rights conferred on them by TOTAL's BCRs : the content of TOTAL's BCRs is published on the Group's corporate Intranet while a summary of the BCRs is available on the Group's website. This summary indicates that the Data Subjects may obtain a complete version of TOTAL's BCRs and the list of the TOTAL Subsidiaries bound by them by sending an e-mail to : data-protection@total.com

Furthermore, TOTAL does not process any Data without informing the Data Subject in advance, expect where doing so :

- Turns out to be impossible, or
- Would involve disproportionate efforts in relation to the interests at stake.

TOTAL informs the Data Subjects about the characteristics of the Processing, in particular about the identity of the Data Controller, the purpose of the Processing, the Data Recipients of the collected Data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and about international Data Transfers. TOTAL also informs the Data Subjects about their rights and about the name of the department or of the person to contact in order to exercise their rights.

Where the Personal Data have not been obtained directly from the Data Subjects, TOTAL informs them at the time of the recording of Personal Data. If disclosure of the Data to a third party is envisaged, TOTAL informs the Data Subjects no later than at the time when the Data are first disclosed.

## V. THE DATA SUBJECTS MUST HAVE A RIGHT OF ACCESS, OF RECTIFICATION AND OF OBJECTION TO THE PROCESSING

TOTAL values the rights of the Data Subjects and enables them to exercise their rights. Only the Data Subjects whose Personal Data originate from the EEA enjoy the following rights.

### A. RIGHT OF ACCESS TO THE DATA

Any Data Subject has the right to obtain from the Data Controller confirmation as to whether or not Data relating to him/her are being processed. He/she has a right of access to his/her Personal Data in accordance with Applicable Law and can obtain from the Data Controller a copy in an intelligible from of the Data undergoing Processing.

The Data Subject also has a right of information as to the purposes for automated Processing.

TOTAL shall respond to any access request without undue delay, depending on the nature of the request and on the interests at stake, within the limits permitted by Applicable Law.

### B. RIGHT TO RECTIFY AND ERASE DATA

Any Data Subject may request that a Data Controller rectify, erase or block Personal Data, in particular if it is inaccurate, incomplete or obsolete.

Where Third Parties have access to the Data, TOTAL shares with them Data that takes into account such rectification, erasure or blocking.

### C. RIGHT TO OBJECT TO THE PROCESSING

Any Data Subject has the right to object on legitimate grounds relating to his/her particular situation to the Processing of Data relating to him/her, save where otherwise provided by Applicable Law.

Any Data Subject has the right to object to the Processing of Personal Data relating to him/her for the purposes of direct marketing.

### D. EXERCISING ONE'S RIGHTS

Any Data Subject may send a request the contact persons as indicated in the information notice about the Processing of his/her Personal Data in order to ask a question about such Processing, to exercise his/her rights.

If a Data Subject believes that a TOTAL Subsidiary has not complied with TOTAL's BCRs, he/she may file a complaint to : data-protection@total.com (see APPENDIX 2).

## VI. THE DATA SUBJECTS MUST NOT BE SUBJECT TO A DECISION THAT SIGNIFICANTLY AFFECTS THEM AND THAT IS BASED SOLELY ON AUTOMATED PROCESSING

Any Data Subject whose Personal Data originate from the EEA must not be subject to a decision that produces legal effects concerning him/her or significantly affects him/her and that is based solely on automated Processing of Personal Data intended to evaluate certain personal aspects relating to him/her, 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.

## VII. THE DATA MUST BE SECURE AND REMAIN CONFIDENTIAL

### A. IMPLEMENTATION OF DATA SECURITY MEASURES

TOTAL implements appropriate measures to guarantee the security and the confidentiality of Data, including Personal Data.

TOTAL has put in place a Policy for the security of information resources, which contributes to the security of the information and of the Data, and a Policy for the security of information systems pursuant to which appropriate technical measures are implemented to guarantee the security and the confidentiality of the Data. In that respect, TOTAL ensures throughout the Processing that the Personal Data remain confidential and are accessed only by individuals authorized for such access due to the nature of their role within the Group (in particular the individuals in charge of implementing the Processing). Only relevant and necessary Data are disclosed to these authorized persons.

The Employees and the staff of third party companies acting on TOTAL's behalf are informed of the conditions that apply to the use of information and communication systems in the Terms of Use of computer resources that are at their disposal and may be consulted at any time.

TOTAL implements appropriate organizational, administrative and technical measures to protect Personal Data against :

- Accidental or unlawful destruction ;

- Loss ;

- Alteration ;

- Unauthorized disclosure or access, in particular where the processing involves the transmission of Data over a network ;

- All other unlawful forms of Processing.

TOTAL implements such measures to ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data, having regard to the state of art and the cost of their implementation.

### B. TOTAL'S CONTRACTUAL COMMITMENT WITH ITS SERVICE PROVIDERS

When calling upon the services of a Service provider, TOTAL makes sure that the latter offers sufficient guarantees as regards the security and confidentiality of Personal Data. The Service Provider shall commit contractually to process Personal Data exclusively under TOTAL's instructions and to guarantee the security and confidentiality of the Data.

The Data protection principles referred to herein are intended to be annexed to all agreements that TOTAL signs with its Service Providers when they process Personal Data originating from the EEA.

When a TOTAL Subsidiary calls upon the services of a Service Provider for Processing Personal Data, the latter must sign a Processing agreement with the TOTAL Subsidiary for which it will act, which must provide that :

- The Service Provider shall act only under instructions from the TOTAL Subsidiary concerned ;

- The Service Provider shall implement appropriate measures to protect the security and confidentiality of the Personal Data.

## VIII. INTERNATIONAL DATA TRANSFERS MUST HAVE A LEGAL BASIS

TOTAL does not transfer Personal Data 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 TOTAL Subsidiary has formally subscribed to the BCRs, or the Transfer relies on another legal instrument recognized by the European Commission as providing an adequate level of protection, such as the Standard Contractual Clauses.

TOTAL does not transfer Personal Data from a country of the EEA directly to a company not belonging to the Group 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, 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 located in a Third Country which does not provide an adequate level of Data protection (either an External Data Controller or Processor), the Data Importer shall enter into an agreement with this other company whereby it commits to observe the principles of TOTAL's BCRs.

# GOVERNANCE

## I. SETTING-UP A NETWORK OF PERSONAL DATA PROTECTION WITHIN THE TOTAL GROUP

TOTAL has put in place a network of Personal Data protection in charge of implementing and properly applying the BCRs within the Group.

- **Corporate Data Privacy Lead (« CDPL »)**

The CDPL manages and coordinates the compliance actions at Group level. To that end, he carries out the same duties as the Branch Data Privacy Lead (« BDPL ») mentioned hereunder. In addition, he is notably responsible for :

- Steering the network of BDPL ;
- Consolidating the reporting of the BDPL ;
- Running the communication and training initiatives within the Group ;
- Advising the managers of the Group about compliance actions and strategies ;
- Submitting an annual report about the compliance status of the Group regarding Personal Data protection.

- **Branch Data Privacy Lead (« BDPL »)**

The BDPL manage and coordinate the compliance actions within their Branch. In particular, he is responsible for :

- Monitoring the implementation of compliance actions ;
- Ensuring the smooth regular communication between the actors involved in Personal Data Protection ;
- Running training initiatives ;
- Handling the requests of all the various actors, in particular of the Data Controllers ;
- Ensuring compliance reporting vis-à-vis the Group's Subsidiaries and the headquarters ;
- Managing the complaint handling procedure.

They put in place within their Branches, a network of Data Privacy Liaison which constitutes together an effective network in charge of locally assisting the functions that may have to process Personal Data.

## II. UPDATING BCRs

TOTAL's Employees have access at any time to TOTAL's BCRs. In addition, Employees may request the list of the TOTAL Subsidiaries that have adopted them by sending an e-mail to : data-protection@total.com

TOTAL's BCRs and the list of the TOTAL Subsidiaries that have adopted them are updated in compliance with internal governance procedures. Such update involves the participation of the BDPL.

Regularly, the CDPL summons the decision-making bodies and invites them to assess the opportunity to update TOTAL's BCRs. If need be, he registers and keeps a record of the updated BCRs and of the list of TOTAL Subsidiaries that have adopted them. He makes them available to the TOTAL Subsidiaries and to the Data Subjects, and forwards them to the TOTAL Subsidiaries and to the Data Subjects, and forwards them to the National Supervisory Authorities upon request.

## TRAINING PROGRAM

In order to ensure a high level of protection of Personal Data within the Group, TOTAL implements a training program designed for all Employees, in particular for the staff who have permanent or regular access to the Data, or who implement the Processing within the Group, or who are in charge of developing tools for the Processing of Personal Data.

This training program consists of various modules to train the Employees on Data protection issues. According to their role within the TOTAL Group, the Employees concerned are invited to attend one or more general or specific training sessions.

- **Level 1 training**

**Objective** : level 1 training aims at raising the general awareness amongst Employees of Data protection issues.

**Target** : this training module is developed for all of the TOTAL Group's Employees. Where relevant, it may also be made available to suppliers, in order to train the staff acting on behalf of TOTAL Subsidiaries.

**Facilities** : this training can be given in any appropriate way, such as, for example, an e-learning module accessible via the TOTAL Group Intranet.

**Content** : level 1 training mainly focuses on the following key themes :

- Stakes in Personal Data protection ;
- Legal definitions : Personal Data, Processing of Personal Data, Data Subjects, Data Controller, Data processor, Transfer of Data ;
- Legislative framework : EU legislation, international legislative framework ;
- Data protection principles derived from the BCRs of the TOTAL Group ;
- Best practices and attitudes ;
- Governance of Personal Data protection within the TOTAL Group ;
- Risks and penalties.

- **Level 2 training**

**Objective** : this second training level aims at training the actors involved with Personal Data protection, to ensure that they develop the required knowledge and expertise for the performance of their duties.

**Target** : this training is developed for all the Employees of the TOTAL Group who are involved in the Processing of Personal Data in the course of their ordinary activities (e.g., payroll manager, client account manager, buyer, IT project manager) and for the actors dealing with the Data protection compliance program (e.g., Corporate Data Privacy Lead, Branch Data Privacy Lead and any Employee, who may assist them in their missions). It may also be made available to service providers, in order to train the staff acting on behalf of TOTAL Subsidiaries.

**Facilities** : this training requires beforehand to have done the level 1 training. Its duration, its contents and its medium vary according to the target and the problems which it faces.

**Content** : level 2 training mainly focuses on the following key themes.

- Legislation in force ;
- More detailed examination of the fundamental principles (legal definitions and legal Data protection principles) ;
- BCRs of the TOTAL Group and Standard Contractual Clauses ;
- Governance of the Data protection compliance program within the TOTAL Group ;
- Best practices and attitudes ;
- Specific process (e.g., complaint handling) ;
- Duties of the actors dealing with governance ;
- Impact assessment procedure ;
- « Privacy by Design » ;
- Compliance reporting ;
- Compliance tools ;
- Case studies ;
- Documentation and resources.

Level 1 and 2 training sessions are regularly updated to reflect regulatory changes and new developments regarding the BCRs and/or the specific features of the TOTAL Group.

## SECURITY

Within the TOTAL Group, a set of reference texts ensures the security and confidentiality of Personal Data. These texts fully apply as part of the implementation of the BCRs of the TOTAL Group. They are listed below.

### 1) Usage Charter for Information Technology and Communication Resources

This document, or the equivalent texts depending on the TOTAL Subsidiaries concerned, requires users to act in accordance with the law and confidentiality rules.

### 2) The Group's information systems security policy

This document applies to all TOTAL Subsidiaries in accordance with their respective decision-making rules. It identifies the method of governance of information systems security within the TOTAL Group.

### 3) Security reference framework of the Group's information systems

This document applies to all TOTAL Subsidiaries in accordance with their respective decision-making rules. It includes 19 different topics.

- Governance of the information systems security ;
- Classification of the information systems resources ;
- Information systems risk mapping ;
- Project, application and infrastructure security throughout their life cycle ;
- Outsourcing of services relating to information system resources ;
- Business continuity of information system resources ;
- Security events management ;
- Safety and physical security ;
- Digital media security ;
- Management of computer evidence ;
- Protection against malicious code ;
- Logical access controls ;
- Platform security ;
- Workstation security ;
- Mobile computing security ;
- Network security ;
- Web browsing protection ;
- E-mail security ;
- Telephony security.

### 4) Directive on information protection

This Group Directive sets out the requirements for the protection of the confidentiality, integrity, availability and control of the information contained and shared within the Group.

These reference texts for security and confidentiality are likely to change in order to reflect the risks faced by the TOTAL Subsidiaries in the context of their activities.

Their implementation is subject to internal control and audit procedures.

Furthermore, the in-house training catalogue lists specific security and confidentiality training modules, including :

- Security architecture ;
- Security for IT Project Managers ;
- Introduction to security, information systems and data protection ;
- Information Assets Security Officer ;
- Information Systems Security Officer.

# IMPACT ASSESSMENT PROCEDURE

## I. OBJECTIVES OF THE IMPACT ASSESSMENT PROCEDURE

Prior to the Processing of Personal Data, the Data Controller within the TOTAL Group shall carry out an assessment of any potential impacts that the Processing might have on Data Subjects. The impact assessment procedure ensures that TOTAL Subsidiaries that have adopted the BCRs achieve compliance with them, particularly when defining the framework and general and detailed operational specifications, and thus maintain a good balance between the Group's interests and those of the Data Subjects. This methodology known as « Privacy by Design » contributes to effective compliance of the Processing operations with the BCRs and helps to guide TOTAL's action regarding the protection of Personal Data.

## II. IMPLEMENTATION TOOL FOR THE IMPACT ASSESSMENT PROCEDURE

This impact assessment procedure relies on a tool known as the « Privacy Impact Assessment Tool » (« PIAT ») which helps the Data Controller to assess the impacts of the Processing on the protection of Personal Data. It also allows the Data Controller to propose solutions, document the existing operations and easily incorporate any changes in the internal or external environments.

## III. NATURE OF THE IMPACT ASSESSMENT

The Impact assessment procedure consists of an assessment of the Processing of Personal Data in accordance with the following legal criteria :

- Entities concerned (legal entity or internal entity) and country concerned ;
- The person responsible for the assessment and the person responsible for the Processing ;
- Purposes of the Processing ;
- Reasons for, and legal basis of, the Processing ;
- Categories of Data Subjects ;
- Estimate of the population concerned (estimated number of people) ;
- Categories of Data processed (including Sensitive Data, if any) ;
- Countries and TOTAL Subsidiaries which first collected the Data ;
- Data Recipients or categories of Data Recipients ;
- Recipient countries and recipient TOTAL Subsidiaries.

## IV. COMPLIANCE ACTIONS

The impact assessment procedure initiated through the PIAT will produce recommendations that will facilitate the compliance of the Processing operations evaluated. The TOTAL Subsidiary, which is the Data Controller, then implements these recommendations, or where deemed necessary, can seek the advice of the BDPL within its entity or business division.

# COMPLAINT HANDLING PROCEDURE

## I. INTERNAL COMPLAINT HANDLING PROCEDURE

TOTAL implements an internal complaint handling procedure as described in APPENDIX 2, to enable every Data Subject to file a complaint with the Group, stating that a TOTAL Subsidiary has failed to observe TOTAL's BCRs.

The TOTAL Subsidiaries cooperate and assist one another for the purposes of handling complaints. In particular, the network of BDPL prepares a report of how complaints are handled with a view to improving the follow-up and the handling of the complaints. This report mentions in particular the number of, and reasons for, complaints, and the timeframe for handling them.

## II. LIABILITY SCHEME

Any Data Subject has a right to judicial remedy in the case of a breach of the rights guaranteed to him/her by Applicable Law and/or TOTAL's BCRs. Any Data Subject who has suffered damage as a result of a breach of TOTAL's BCRs is entitled to receive compensation for the damage suffered.

Any Data Subject can assert the protection principles mentioned in TOTAL's BCRs to :

- The court of the EEA country where the Data Exporter is established ; or
- The National Supervisory Authorities.

Within the TOTAL Group, any Subsidiary that has subscribed to TOTAL's BCRs is responsible for their observance, as well as for observing Applicable Law. 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 shall commit to take over the settlement of disputes that may arise in the EEA. The Data Exporter agrees therefore to be liable vis-à-vis the Data Subject and, in case of actual damage, to pay compensation to the Data Subject for any harm suffered as a result of the violation of TOTAL's BCRs.

If a Data Subject claims compensation in the case of a breach of these Rules by a Data Importer, the Data Exporter Is responsible for demonstrating that the Data Importer has not violated TOTAL's BCRs.

## III. COOPERATION BETWEEN TOTAL AND SUPERVISORY AUTHORITIES

Any TOTAL Subsidiary that has subscribed to the BCRs commits itself to consult the competent supervisory authority and to follow its recommendations regarding the international Transfers of Data in the event of a complaint or of a particular request from such authority. Any TOTAL Subsidiary that has subscribed to the BCRs accepts to be audited by the supervisory authority of its country of establishment.

# INTERNAL CONTROL AND AUDIT

## I. EXISTENCE OF INTERNAL CONTROL AND AUDIT SYSTEM

TOTAL's BCRs require the implementation of internal control and audit systems. These systems ensure the proper implementation of all the BCRs by TOTAL Subsidiaries at frequent intervals, according to the priority areas identified by the CDPL or the BDPL.

The resulting audit plan shall give Supervisory Authorities the right to carry out Data protection audits themselves if required. In accordance with the Intra-Group agreement, each signatory TOTAL Subsidiary undertakes to submit to such audits, as carried out by the competent supervisory authority of its country of establishment.

The results of the internal controls or audits are communicated to the CDPL and are made available to the competent Supervisory Authority.

## II. INTERNAL CONTROL SYSTEM

### A. DESCRIPTION OF THE INTERNAL CONTROL SYSTEM

The BDPL conduct assessments of the level of compliance with TOTAL's BCRs within their division or the relevant TOTAL Subsidiaries at regular intervals or on specific request from the CDPL. These assessments are specific to the business processes of each division or the relevant TOTAL Subsidiaries (HR, marketing, sales, etc.).

The frequency of these assessments must be adapted to :

- The scope of the relevant business process (e.g., a process that is national in scope or a multi-country process) ;
- The number of Data Subjects ;
- The various categories of Data processed ;
- The eventual Processing of Sensitive Data.

### B. TYPES OF ASSESSMENTS

The assessments can be full or partial. Full assessments cover the entire business process and all aspects of any associated Data Processing. Partial assessments only focus on a segment of the business process, due to its sensitivity or other specificities. Such is the case for instance, with the review of the technical and organizational measures to ensure the protection of Data processed, even momentarily, by a Data Recipient, when providing services. Partial assessments thus allow the control of the most sensitive aspects of Processing operations in an effective and efficient way.

### C. ANNUAL INTERNAL CONTROL PLAN

Each division or TOTAL Subsidiary develops, through its BDPL, its annual internal control plan. This plan must include at least a full assessment of two significant business processes. In addition, the plan provides for the self-assessment of five computer applications or active projects per year.

Moreover, within the framework of the internal control system, the BDPL check the existence and monitor the implementation of the action plans resulting from the assessments.

Finally, the BDPL measure the rate of internal participation in training (e.g., e-learning) and take actions to increase this participation rate.

## III. INTERNAL AUDIT SYSTEM

### A. DESCRIPTION OF THE AUDIT PROGRAM

The internal audit focuses exclusively on the internal control system. It is carried out by the Group Internal Audit Department of TOTAL S.A. Following a risk analyses and/or proposal from the operational entities or various functional departments, the internal entities, business processes, computer systems or applications which are scheduled to be audited in the ensuing period are identified.

To that effect, the following factors are taken into consideration :

- The amount of Data processed ;
- The novelty of the activity in question ;
- Significant changes to the activity in question ;
- The outsourcing of the activity ;
- Identified particular problems ;
- Object unaudited for a number of years.

### B. PLANNING

The audit plan leads to the scheduling of audit assignments. This planning takes into account :

- The availability of the key persons to meet within each entity concerned ;
- Operational constraints ;
- Ongoing projects.

The establishment of audit assignments includes the identification of internal or external resources assigned to the audit teams, as well as the development of their management.

### C. IMPLEMENTATION OF CORRECTIVE ACTIONS AND FOLLOW-UP OF RECOMMENDATIONS

The management of the TOTAL Subsidiary responsible for the audited object shall implement corrective actions, if necessary.

A follow-up of the implementation of the corrective actions is communicated to the CDPL. An audit of the implementation of the corrective actions may be carried out if necessary.

### D. REVIEW OF THE EFFECTIVENESS OF THE SYSTEM

As part of its duties, the Group Internal Audit Department conducts internal audit reviews to verify the effectiveness of the global internal control system.

Moreover, the effectiveness of the overall internal control system is ensured by a regular reporting of the results of the internal audits, including the implementation of the internal auditors' main recommendations to the Chairman and Chief Executive Officer, the Executive Committee and the Audit Committee of TOTAL S.A. This direct exchange with the Chairman of the Audit Committee strengthens the internal audit function's independence.

## APPENDIX 1

## THIRD PARTY BENEFICIARY RIGHTS

TOTAL's BCRs grant rights to Data Subjects to enforce the Rules as third-party beneficiaries, as detailed in the various chapters of these BCRs.

More specifically, they may enforce the following principles according to the terms and conditions set out in these 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) Procedure for handling complaints

Within the Group, the BDPL are responsible for responding to complaints, with the help of the TOTAL Subsidiaries. In particular, each complaint will be examined by the appropriate BDPL before being forwarded to the legal department of the TOTAL Subsidiary acting as the Data Controller to be investigated. The complaint may also ber e-directed to the relevant department of any other TOTAL Subsidiaries, if necessary, to handle the compliant. The TOTAL Subsidiaries shall cooperate and assist one another for the purposes of handling complaints.

### 3) TOTAL's response

Within three months of TOTAL receiving a complaint, the appropriate 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 TOTAL's BCRs if necessary.

The appropriate BDPL shall send a copy of the complaint and any written reply to the CDPL.

### 4) 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.

## SCHEMA : INTERNAL COMPLAINT HANDLING PROCEDURE