DATA SECURITY STANDARDS

PRIVACY AT FCC GROUP

ID Code:	**NRM-12-EN**
Version:	1.0
Classification:	FCC_INTERNAL_USE

INDEX

PURPOSE

The purpose of this Standard is to specify the main guidelines and requirements that all FCC Entities must observe and fulfill on the processing of Personal Data.

SCOPE

a. Geographical

This Standard applies to FCC Entities located in any State/Country/World Region (hereinafter FCC Entities) that they are included in the following cases:

- Those Entities in which FCC holds a majority stake.
- Those Entities that despite not having a majority stake, FCC holds the management.

b. Material

This Standard applies to all information containing Personal Data (processed in paper and/or digital media) that is collected, managed or transferred by the employees of FCC Entities or their Partners and/or Providers.

DEFINITIONS

(a) 'Personal Data': any information relating to an identified or identifiable natural person ('Data Subject'); 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 physical, physiological, mental, economic, cultural or social identity;

(b) 'Processing of personal data' ('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;

(c) 'Data Controller': the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

In this sense, each FCC Entity will be responsible for the file containing personal data it manages (e.g. Employees, Customers and Providers).

(d) 'Data Processor': the natural person or legal entity, public or private, or administrative body that, alone or jointly with others, processes personal data on behalf of the data

controller, due to the existence of legal relations binding them and delimiting the scope of his action for the provision of a service.

(e) 'Data subject's consent': any free, unequivocal, specific and informed indication of his wishes by which the data subject consents to the processing of personal data relating to him.

(f) 'Data with special protection': personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.

(g) 'Erasure': procedure through which the data controller stops using data. Erasure shall imply data being blocked, comprising their identification and retention in order to prevent processing with the exception of being at the disposal of public Administrations, Judges and Courts for the purpose of determining any liability arising from processing, and only for the duration of such liability. On the expiry of such term, the data shall be deleted.

VALUES ON PERSONAL DATA PROTECTION

The FCC Group is a constantly evolving group that advocates the use of the latest information systems and technological advances. In practice, this means that the information can be stored and processed in large quantities and in a short time.

Therefore, the FCC Group is constantly concerned about confidentiality, security and proper use of the information managed in their daily processes and, in particular, its Employees, Customers and Providers' Personal Data.

For that reason, the FCC Group manages the processing of Personal Data based on the following values:

- Transparency and trust regarding the secure processing of Personal Data at all times.
- Responsibility and commitment for the use of Personal Data based on their confidentiality.
- Efficiency in the secure management of Personal Data.
- Availability of Personal Data when it is necessary and only by the person who need it because of their functions.
- Integrity of information to avoid tampering.

GENERAL PRINCIPLES ABOUT PERSONAL DATA MANAGEMENT

Each FCC Entity must manage the Personal Data in accordance with the following principles:

- Principle of Subjet's Consent

The Personal Data can only be processed by the FCC Entity or communicated to another Entity or Body if the Data Subject had previously given their consent. Nevertheless, it will be possible the processing or communication of Personal Data without the Subjet's consent when it is authorized by a national law or it is necessary for the management and maintenance of the Data Subject's contract.

- Principle of Information to the Data Subject

From prior to any collection of Personal Data, the FCC Entity must inform to the Data Subject in an evidencing way, at least, about the identity and address of the FCC Entity, existence of a file or personal data processing, purposes of collecting and processing of Personal Data, recipients of the information when the information is communicated to another person (different of his Data Subject), and about the possibility of exercising his rights of access, rectification, erasure and objection of Personal Data.

- Principle of specific purpose on the collecting

The Personal Data managed by the FCC Entity only must be collected and processed for specified and explicit purposes and this information must be always adequate, relevant and not excessive in relation to the purpose for which was collected.

- Principle of Quality

The Personal Data managed by the FCC Entity must be accurate and updated in such a way as to give a true picture of the current situation of the Data subject. When the FCC Entity has fulfilled the purpose for which they were collected, this information must be erasure.

- Principle of Security of processing

The FCC Entity must ensure the confidentiality of Personal Data, the access to them only by authorized personnel and the correct implementation about technical and organizational measures according to the type of Personal Data to prevent accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

- Principle of Legality

In any case and in addition to that specified above, the Personal Data managed by the FCC Entity must be used in a lawful way and in accordance with the purpose for which they were collected, according to the national law currently in force in each State/Country/Region.

PROCESSING GUIDELINES

1. Organization and Responsibilities on Privacy

On Privacy, the Group FCC has adopted an organizational structure with defined roles and responsibilities:

a.1 Organizational Structure:

- Information Security and IT Risk Department: This is the highest figure in the management and coordination on Privacy in the FCC Group.
- Data Protection Coordinator: It is the greatest figure in the management and coordination on Privacy within the area of his responsibility.

- Security Officer: Is the greatest figure in the management and coordination on Privacy within the FCC Entity that is responsible.

If deemed appropriate, the Information Security and IT Risk Department proceed to the creation and/or modification of the above described figures.

a.2 Roles and Responsibilities:

The roles and responsibilities for each figure are the following:

- Information Security and IT Risk Department:

  - Specify the main guidelines on Privacy in FCC Group.
  - Manage, implement and coordinate the security measures and requirements on Privacy in FCC Group.
  - Support the other figures on the implementation of the requirements on Privacy in FCC Group.

- Data Protection Coordinator:
  - Manage, implement and coordinate the necessary actions within his area of responsibility.
  - Support the Information Security and IT Risk Department and the Security Officer within his area of responsibility.
  - Report regularly to Information Security and IT Risk Department, the measures implemented in his area of responsibility.
  - Report immediately any security incident or breach about Personal Data to the Information Security and IT Risk Department and any communication or request for information required from the Supervisory Authority on Data Protection.

- Security Officer:
  - Manage, implement and coordinate the necessary actions on Privacy within FCC Entity that is responsible.
  - Support the Information Security and IT Risk Department and the Data Protection Coordinator of his area in fulfilling the necessary requirements on Privacy within FCC Entity that is responsible.
  - Report regularly to the Data Protection Coordinator of his area about the requirements implemented on Privacy within FCC Entity that is responsible.
  - Report immediately any security incident or breach about Personal Data to the Information Security and IT Risk Department, and any communication or request for information required from the Supervisory Authority on Data Protection.

2. Processing of Sensible Data

It is not allowed for the FCC Entities any processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and the processing of data concerning sex life.

In any case, for the processing of Personal Data about health and about trade union membership, the FCC Entity will need the Data Subject's expressed consent, previous and in written form (except in cases where the law of the State in which FCC Entity is located provides that is necessary the Data Subject's consent always).

3. Data Protection Agreement

If it was necessary to contract certain services to an external Entity or to any other FCC Entity (hereinafter Data Processor) under which it can/need access to Personal Data, the FCC Entity must choose a Provider that has implemented the necessary security measures in accordance with the type of data and sign a previous Data Protection Agreement. In that Agreement, FCC Entity must expressly specify that:

- The Data Processor shall act according to the FCC Entity instructions.
- The Data Processor shall not use the Personal Data for other purposes than that contained in the Agreement.
- The Data Processor shall not communicate the Personal Data to other parties, even to preserve.

To prepare the Data Protection Agreement, the Legal Department of each FCC Entity must use the Data Protection Agreement Template that the Data Protection Coordinator provides. The Legal Department of each FCC Entity must review that the agreement is according to the requirements of the each national law currently in force.

All Data Protection Agreement signed with a Data Processor must be reported immediately to the Data Protection Coordinator.

4. International Transfer of Data

Whenever a FCC Entity has to transfer Personal Data to another FCC Entity and/or public/private Body located in another country, the FCC Entity exporter must review and comply with specific requirements of each national law currently in force. This national legislation may require obtaining the previous authorization of the Supervisory Authority on Data Protection.

In this regard, when the FCC Entity has to transfer Personal Data to another country must notify it to the Data Protection Coordinator.

5. Rights of Access, Rectification, Erasure and Objection

The FCC Entity must manage the exercising rights of Access, Rectification, Erasure and Objection about Personal Data within legal deadlines and legal form required by the national law currently in force.

In this regard and unless the national law currently in force specifies other considerations, the exercise of any of these rights must be answered in writing and within one month for Access rights and within 10 days for the rest rights, counted from receipt of the notification.

6. Audits

FCC Entities must conduct regular audits (internal or external) to verify the correct implementation of this Standard and the correct implementation of security measures.

Before that, the Information Security and IT Risk Department shall provide to the FCC Entity the instructions about the audit and the FCC Entity must report to that Department on the audit conclusions.

7. Reporting Personal Data breach

Any security incident or breach about Personal Data must be reported immediately by the FCC Entity to the Information Security and IT Risk Department.

8. Compliance with Data Protection national law currently in force

This Standard applies directly to each of the FCC Entities, and if the Areas or FCC Entities have their own internal regulations regarding the protection of Personal Data, they must not be at odds with this Standard that will prevail in any case.

Also, the FCC Entity must comply with the specified by its Data Protection national law currently in force.

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever improvements are suggested as a result of audits carried out.
- Whenever there are major technology changes.
- Whenever there are changes to the current legislation regarding the provisions established in this Standard.

The information used for the review of this Standard must be notified to the Information Security and IT Risk Department, who must then notify the Data Security Department Committee of this information.

BREACH OF STANDARD

Any breach of this Standard will be punished according to the disciplinary regulation in force at FCC Group, without prejudice to specify in the national law currently in force of each State/Country in which the FCC Entity is located.

ADDITIONAL CONSIDERATIONS

This Standard will be published in Spanish and in English language and it may be translated into other languages.

The edition in Spanish as the English has official status in the centre where the Spanish or English language is considered official language. Otherwise, it will use the English language edition.

EXCEPTIONS

Any exceptions to the application of this standard must be justified in writing and approved by the Information Security and IT Risk Department.

The way to communicate exceptions will be the email address INFOSECURITY@fcc.es or the usual channels provided by "Service Desk FCC" (Service user) for requests reception.

The person responsible for the exception must be a superior (from Department Manager or Delegate).

To communicate exceptions must be used the following form:

SECURITY POLICY AND STANDARDS EXCEPTIONS	
Petitioner	
Responsible person	
Policy / Standard	
Chapter/Part affected	
Description of exception and justification	

REFERENCES

- DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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. 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.
- The set of guidelines for Information Security FCC Group.

DOCUMENT CHANGE CONTROL

Document Information

FILE NAME:				
VERSION	DATE	CHANGE	AUTHOR	REVIEWED BY
1.0	2013 february	Document creation	Information Security and IT Risks Department	FCC Policy Committee
1.0	October 2019	General Revision	Information Security and IT Risks Department	FCC Policy Committee

Please Note: Hard-copies are not controlled

END OF DOCUMENT