NORMA DE SEGURIDAD DE LA

COMPLIANCE WITH THE REQUIREMENTS OF THE GENERAL DATA PROTECTION REGULATION

Identification code:	**NRM-19-EN**
Version and date:	v1.0 October 2019
Clasification:	FCC_Internal_Use
Recipients:	All FCC Staff and Users

NORMA PARA EL CUMPLIMIENTO DE LOS REQUISITOS DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

INDEX
CONTENT

INTRODUCTION

On May 25, 2016, Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, came into force, regarding the protection of natural persons with regard to the processing of personal data and the free movement of this data (hereinafter General Data Protection Regulation, Regulation or GDPR).

Despite its entry into force in 2016, the GDPR granted a period of 2 years for its effective application in the Member States and introduced a series of changes and developments in data protection that must be applied from May 25, 2018, date from which, its content will be fully applicable.

From the Department of Information Security of FCC - DSIGRT (Department responsible for establishing the minimum guidelines on privacy), and to comply with the European regulations on data protection derived from the GDPR, this "Standard" is developed, which must be applied in each of the FCC Group Entities to adapt them to said regulations with the collaboration of the FCC matrix, the Data Protection Coordinators and the entire structure created for this purpose.

RELEVANT NEWS INTRODUCED BY THE REGULATION

The Regulation establishes a series of developments that must be implemented in the FCC Entities that fall within the scope of the GDPR.

For information purposes, and without prejudice to the effective measures to be implemented that are established in point 6 of this Standard ("Minimum Guidelines on Privacy"), some of the novelties of the GDPR are set out below:

1. The principle of "Proactive Responsibility" is established by which each FCC Entity will be responsible for the correct compliance in time with the regulations and must have the capacity to demonstrate it at any time through the implementation of a solid system of evidence.

2. The principles applicable to the processing of personal data are strengthened: legality, loyalty and transparency; collected for specific, explicit and legitimate purposes ("limitation of purpose"); limited to what is necessary in relation to the purposes for which they are processed ("data minimization"); accurate and up to date ("accuracy"); maintained in a way that allows the identification of the owners of the data for no longer than necessary for the purposes of the processing of personal data ("limitation of the retention period"); treated in such a way that adequate security of personal data is guaranteed ("integrity and confidentiality").

3. The requirement of consent is reinforced. One of the fundamental bases for processing personal data is consent. The Regulation requires that the consent, in general, be free, informed, specific and unequivocal. In order to consider that the consent is "unequivocal", the Regulation requires that there be a declaration of the interested

parties or a positive action that indicates the agreement of the interested party. Consent cannot be deduced from the silence or inaction of citizens, but there must be evidence of it.

4. The right to information is strengthened by forcing the Entity to provide more information prior to the collection or registration of the personal data of employees, customers and suppliers by any means.

5. New rights are introduced in favor of the owner of the data, among which it is worth highlighting the right to data portability that allows the owners to request the Entity to deliver or recover such data in a format that allows its transfer to another responsible.

6. The need to comply with data protection from the design is established, which requires compliance with data protection from the start of the service or from the purchase of the system. Techniques such as pseudo-anonymization will be promoted (understood as the processing of personal data so that they can no longer be attributed to the owner of the data without using additional information, provided that such additional information appears separately and is subject to technical and organizational measures aimed at ensure that personal data is not attributed to an identified or identifiable natural person).

7. The obligation to notify the Data Protection Authority is introduced within a minimum period of time and to the holder of the data (in certain cases) about those security breaches on the data that occur and that pose a risk of damages for the Physical persons. All security violations must be documented.

8. The need to establish technical security measures based on risks that guarantee an adequate level of security is imposed, as well as the obligation to perform impact assessments on data protection (hereinafter, PIAs), whenever it is probable that treatment operations, especially when new technologies are used, entail a high risk for the rights and freedoms of natural persons or in the types of treatments indicated by the Control Authority.

9. The concept of “right to be forgotten” is introduced to request that personal data be deleted in certain circumstances.

OBJECTIVE

The objective of this Standard is to transfer to the FCC Entities (which fall within the scope of the Regulation) the main novelties introduced by the Regulation, as well as the actions and minimum requirements that must be met by each FCC Entity.

Notwithstanding the foregoing, the FCC Group may develop procedures that develop and detail certain points of this Standard.

Note: The Privacy Policy in the FCC Group is still in force.

SCOPE

a. Geographical

This Standard is applicable and mandatory by the Entities that belong to the FCC Group located in any State / Country / Region of the European Union, more specifically:

• Those Entities in which FCC has the majority participation (plus 50%).
• Those Entities that in spite of not having FCC the majority of participation, if it shows the management or administration of the same.

b. Material

This Standard shall apply to all information with Personal Data (on paper support and / or computer support) responsibility of the FCC Entities that is collected, accessed, managed, transferred or in any other way treated by the staff of the FCC Entities or its Partners and / or Suppliers.

DEFINITIONS

1) "Personal data" means any information about an identified or identifiable natural person ("the interested party"); Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of the identity itself physical, physiological, genetic, psychic, economic, cultural or social of said person.
2) "Treatment" means any operation or set of operations carried out on personal data or personal data sets, whether by automated procedures or not, such as collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other means of enabling access, collation or interconnection, limitation, deletion or destruction.
3) "Pseudonymization" means the processing of personal data in such a way that it can no longer be attributed to an interested party without using additional information, provided that such additional information appears separately and is subject to technical and organizational measures aimed at ensuring that personal data are not attributed to an identified or identifiable natural person.
4) "File" means any structured set of personal data, accessible according to certain criteria, whether centralized, decentralized or distributed in a functional or geographical way.
5) “Responsible for the Treatment” or “Responsible”: the natural or legal person, public authority, service or other body that, alone or together with others, determines the purposes and means of the treatment; If the law of the Union or of the Member States determines the purposes and means of the treatment, the person responsible for the treatment or the specific criteria for their appointment may be established by the law of the Union or of the Member States. In this sense, each FCC Entity will be Responsible in relation to the personal data that it manages (e.g. Employees, Customers and Suppliers).

6) "Treatment Manager" or "Person in Charge": the natural or legal person, public authority, service or other body that processes personal data on behalf of the controller.
7) "Consent of the interested party" means any manifestation of free, specific, informed and unambiguous will by which the interested party accepts, whether by means of a statement or a clear affirmative action, the processing of personal data concerning him.
8) "Violation of the security of personal data" means any breach of security that causes the destruction, loss or accidental or unlawful alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to said data. data.
9) "Health-related data" means personal data relating to the physical or mental health of a natural person, including the provision of health care services, that reveal information about his or her state of health.
10) «Data protection coordinator»: Is the person belonging to an FCC Group Entity, appointed to coordinate the data protection actions of an area of the FCC Group.
11) "Responsible for the Entity or Security Entities in the field of Data Protection": Is the person belonging to an Entity of the FCC Group, appointed to manage the data protection actions of one or more Entities of the FCC Group.

GUIDELINES ON DATA PROTECTION

The minimum guidelines that must be observed and complied with by each FCC Entity are detailed below, without prejudice to compliance with the requirements demanded by any other Data Protection regulations that may apply (by law in the country where that the FCC Entity is domiciled or located).

1.1 FCC Privacy Structure

In order to comply with all the regulations derived from the Regulations, from the FCC Group an organizational structure has been created to decide, coordinate, implement and supervise data protection matters throughout the Group.

Said structure must be formed, as a minimum, by:

- Privacy Board: Multidisciplinary body of the highest level in the FCC Group on Privacy. It is formed by: Legal Counsel Director, Human Resources Director, FCC Internal Audit, Risk Management and Compliance Department Director, Director of the Information Systems and Technologies Division and the Data Protection Coordinator of the FCC Group.

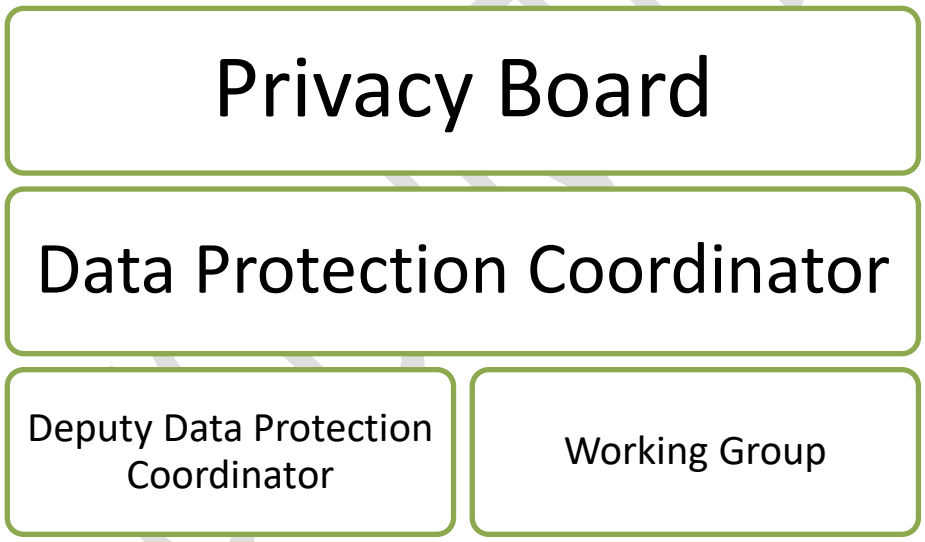
- Data Protection Coordinator of the area: Person belonging to an area of the FCC Group and designated by said area to promote, implement, coordinate and manage within the FCC Entities that belong to it, the necessary actions to fulfill the obligations in terms of privacy. It will be national and / or international. Likewise, an Area Data Protection Coordinator may be appointed for a certain country / s in particular, in any case dependent on the Area Data Protection Coordinator. For the purposes of this document, the following are considered Areas: FCC Corporation,

FCC Construction, FCC Environmental Services, FCC Water Services and Cementos Portland Valderrivas Group.

- Deputy Data Protection Coordinator: For the assistance of the Data Protection Coordinator of the area, the Deputy Coordinators deemed necessary within each activity area may be formally appointed.

- Working Group: With the exception of a duly justified exception to the Privacy Board, within each area a Work Group should also be created consisting of those responsible for the Group's Departments (local authorities of each Entity, Delegation or zone) that have the greatest impact on Privacy, by the Data Protection Coordinator of the area (and the attached Coordinators and / or the country that have been appointed) and constituted with the purpose of promoting, coordinating, implementing, managing, discussing issues related to the protection of data that take place within the area of activity and verify the correct adaptation to the Regulation and the local regulations of Data Protection that are applicable in the FCC Entities that are within its area of activity.

The organizational structure of Privacy for each of the areas will be, where appropriate, the following:



For the functions and responsibilities of each figure, see the document “Government Model on Privacy”.

1.2 General Principles of Action

The following are the general principles regarding privacy that must be observed and complied with for the processing of personal data:

a) Treated in a lawful, loyal and transparent manner in relation to the owner of the data ("legality, loyalty and transparency").

b) Collected for specific, explicit and legitimate purposes, and will not be treated further in a manner incompatible with those purposes; The subsequent processing of personal data for archival purposes in the public interest, scientific and historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes ("limitation of purpose").

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization").

d) Exact and, if necessary, updated; All reasonable measures will be taken to eliminate or rectify, without delay, personal data that are inaccurate with respect to the purposes for which they are processed ("accuracy").

e) Maintained in a way that allows the identification of the owners for no longer than necessary for the purposes of the processing of personal data; personal data may be kept for longer periods provided that they are processed exclusively for archival purposes in the public interest, scientific or historical research purposes or statistical purposes, without prejudice to the application of appropriate technical and organizational measures imposed by this Regulation to in order to protect the rights and freedoms of the interested party ("limitation of the conservation period").

f) Treated in such a way as to ensure adequate security of personal data, including protection against unauthorized or unlawful treatment and against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures ('integrity and confidentiality »).

g) When the processing is based on the consent of the owner of the data, the FCC Entity must be able to demonstrate that he consented to the processing of his personal data.
h) If the consent of the holder is given in the context of a written statement that also refers to other matters, the request for consent will be presented in such a way that it is clearly distinguished from other matters, in an intelligible and easily accessible form and using a clear and simple language.

1.3 Organizational Aspects

At the organizational level, at least the following actions must be carried out:

A. ESTABLISHMENT AND APPOINTMENT OF THE MODEL OF GOVERNANCE IN THE AREA OF PRIVACY IN EACH AREA

Within each of the areas of activity, a Government Model on Privacy will have to be formally designed and appointed, which must have at least one Data Protection Coordinator in the area of activity (national and / or international). In addition, the Deputy and / or Country Coordinators that are deemed necessary may be appointed within each area.

In all cases there must be a formal appointment and the functions and responsibilities assumed by each of the appointed positions must be well defined.

The appointments made, as well as any changes made in the Government Model (be it changes in responsibilities, appointments, etc.) must be reported to the Area Data Protection Coordinator and the DSIGRT.

B. CONTROL AND UPDATED INVENTORY OF FCC ENTITIES OF EACH AREA

Each Area Data Protection Coordinator must keep control of the FCC Entities in their area at all times (and to which this Standard applies), so that the data protection guidelines are applied to them, and for possible inspections or audits.

To this end, the data protection management tool of each area must be kept up to date, incorporating the new FCC Entities that are created or acquired and deregistering those entities that have disappeared or are outside the control of FCC.

C. OBLIGATION TO AVOID THE RIGHT FULFILLMENT OF THE REGULATIONS

Based on the principles of Proactive Responsibility and for possible inspections or audits, all aspects concerning the processing of personal data, the correct compliance with the regulations, as well as the corrective measures that are applied must be evidenced.

That is to say, all actions, policies, measures and even meetings held (by minutes) must be evidenced and guarded by each of the FCC Entities for the keeping and application of this Standard and other actions concerning data protection to which The FCC Group is bound by current regulations.

1.4 Legal Aspects

With regard to legal aspects, at least the following actions must be carried out:

A. RECORDS OF TREATMENT ACTIVITIES

In each FCC Entity it will be necessary to identify and inventory all the points where personal data processing is carried out in order to adapt them to the GDPR.

Said inventory of treatments will also be the basis on which to create the Registry of Treatment Activities required by the Regulation in its article 30.

Said Registry must contain, at a minimum, the information collected in art. 30 GDPR.

It will be the responsibility of each Area Data Protection Coordinator to maintain and maintain, in a diligent manner, the Records of Personal Data Processing Activities.

B. CLAUSED

The clauses and / or contracts for data protection that are used in each FCC Entity (clauses / contracts of Employees, Clients and Suppliers) must be reviewed and updated in accordance with the requirements of the GDPR.

For this, those models of clauses / contracts provided by the DSIGRT will always be taken as a basis. These models must be reviewed according to the requirements required by the Data Protection regulations that may apply.

Specific:

I. EMPLOYEES

All FCC Entities must regulate in accordance with the GDPR (and the requirements that may be established by the applicable Data Protection regulations) the information and consent clauses regarding Data Protection of all current employees.

Likewise, with respect to future employees, the FCC Entities must sign an information and consent clause in accordance with the requirements of the GDPR (and the requirements that may be established by the Data Protection regulations that may apply).

II. CUSTOMERS

All FCC Entities must regulate in accordance with the GDPR (and the requirements that may be established by the applicable Data Protection regulations) the information and consent clauses regarding Data Protection of all current customers.

Likewise, with respect to future clients, the FCC Entities must sign an information and consent clause in accordance with the requirements of the GDPR (and the requirements that may be established by the applicable Data Protection regulations).

III. SUPPLIERS

In the event that it is necessary to contract an application and / or Services to an external Entity or to any other Entity of the FCC Group (hereinafter, Supplier) by virtue of which, the latter may / should access / process Personal Data, the Entity FCC must choose a Provider that offers sufficient guarantees to apply appropriate technical and organizational measures, so that the treatment is in accordance with the requirements of the Regulation and is signed prior to access / management of any data a Service Delivery Contract in which the minimum content that art. 28 GDPR (and the requirements that may be established by the applicable Data Protection regulations). For the preparation of the Service Provision Contract, each FCC Entity shall take as a basis the model of Service Provision Contract provided by the Data Protection Coordinator of the area to which the FCC Entity belongs.

Any Contract for the Provision of Services signed with a Person in Charge of the Treatment must be immediately notified to the Data Protection Coordinator of the area to which the FCC Entity belongs and stored correctly by the area.

Likewise, in all "Request For Proposal" (RFP) and / or offer requests that are drawn up, a Data Protection clause must be included in accordance with the requirements of the GDPR. The model will be provided by the Data Protection Coordinator of the area.

With regard to the contracts in force with Suppliers whose end date is before May 2018, the following is established: In principle, there is no obligation based on the Regulation, because such contracts should already have the Data Protection clause that meets with current regulations. Notwithstanding the foregoing, those contracts that are in this situation but are expected to carry out an extension of their validity, YES must be regularized according to the Regulation.

Regarding the contracts in force with Suppliers whose end date is after May 2018: The signature of the Data Protection clause must be managed, which, at a minimum, will comply with the requirements set forth in art. 28 GDPR (and the requirements that may be established by the applicable Data Protection regulations). The model Data Protection Clause provided by the Protection Coordinator must be taken as a basis.

1.5 Technical Aspects

A. INVENTORY OF INFORMATION SYSTEMS

In each FCC entity it will be necessary to identify and inventory all the information systems (internal and external) through which personal data are processed / managed in order to adapt them and their security measures in accordance with the Regulations.

B. RISK ANALYSIS AND ASSESSMENT OF PRIVACY IMPACT

Taking into account the state of the art, the application costs, the nature, the scope, the context and the purposes of the treatment, as well as risks of variable probability and severity for the rights and freedoms of natural persons, the FCC Entity will apply the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, which may include, among others:

a) pseudonymisation and encryption of personal data (in some cases);

b) the ability to guarantee the permanent confidentiality, integrity, availability and resilience of treatment systems and services. The information system must also guarantee the portability of data, that is, comply with the technical measures that allow to respond to an exercise of a right of data portability through which the interested party will have the right to receive the personal data incumbent on him, provided to FCC in a structured format, for common use and mechanical reading and to be transmitted to another person responsible for the treatment.

c) the ability to restore availability and access to personal data quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of the effectiveness of technical and organizational measures to ensure the safety of the treatment.

In this sense, all the information systems used in the FCC Group must be subject to a risk analysis that allows identifying the necessary security measures in accordance with the above.

Likewise, in accordance with the provisions of article 35 of the Regulation, provided that from any FCC Entity a personal data processing will be carried out that, due to its nature, scope, context or purposes, entails a high risk for the rights and Freedoms of natural persons, an Impact Assessment (PIA) in relation to the privacy of such treatment in the protection of personal data will be carried out before treatment.

In any case, a PIA must be carried out whenever the processing of personal data consists of: a systematic and exhaustive evaluation of personal aspects of natural persons that is based on an automated treatment, such as profiling; a large-scale treatment of the special categories of data referred to in Article 9 of the GDPR; or a large-scale systematic observation of a public access area.

Both the risk analyzes and the Privacy Impact Assessments (PIAs) carried out by the FCC Group will be carried out in accordance with the Risk Assessment Methodology that will be approved by the Privacy Board.

C. AUDITS TO VERIFY COMPLIANCE

The FCC Entities must carry out periodic audits (internal or external) in order to verify the correct compliance with this Standard, the established guidelines and the security measures implemented.

Prior to its realization, the DSIGRT will provide the corresponding instructions for its realization to the FCC Entity and it must report the results of the same to the DSIGRT.

D. NOTIFY SECURITY VIOLATIONS RELATED TO PERSONAL DATA

The FCC Entity will immediately notify, in writing and without prejudice of those notifications that were necessary to the corresponding Control Authority, to the Director of Information Security of FCC (sdseguridad@fcc.es), the existence of any “Violation of Security ”in the sense of any breach of security that causes the destruction, loss or accidental or unlawful alteration, loss and alteration, disclosure or unauthorized access, of personal data transmitted, preserved or otherwise processed or unauthorized communication or access to such data, including the information required in the GDPR and other regulations that may apply.

E. PRIOR CONSULTATION TO AREA DATA PROTECTION COORDINATORS

Whenever from a FCC Entity a new project is to be initiated, a new application is contracted or an activity (commercial, marketing, advertising, or any other type of activity) that may involve the processing of personal data must be consulted beforehand the Data Protection Coordinators of the corresponding area, the impact of said activity or project on data protection.

RESPONSIBILITIES AND CONSEQUENCES OF A BREACH

As established by the FCC Code of Ethics, all employees are responsible for knowing and complying with internal laws and regulations. In any case, the FCC Group will make available the necessary means for them to know and understand their obligations.

Likewise, each FCC Entity (whatever its legal form) is responsible for complying with the obligations and requirements required by the European Data Protection Regulation, by the local Data Protection regulations that may be applicable and with the decisions and instructions sent by the DSIGRT on said matter. This responsibility will extend beyond the date of entry into force of the GDPR.

In general, each FCC Entity is responsible, at a minimum, for:
• The correct adaptation and fulfillment (in term) of the obligations established by the Regulation and the local regulations of Data Protection that are applicable, as well as derived from this Regulation.
• Establish a solid system of evidence that allows it to demonstrate its correct compliance afterwards.
• Communicate to the Data Protection Coordinator of the area any corporate change that may have a reflection on privacy management. This communication must be prior to the effective realization.
• Facing the economic sanctions imposed on them by the Control Authority in case of non-compliance with the requirements of the Regulation and the local Data Protection regulations that may apply.

The legislator has greatly increased the amount of economic sanctions. The imposition of administrative sanctions, the amount of which can reach € 20,000,000 or 4% of the total global annual business volume of the previous financial year (opting for the largest amount), is envisaged in case of non-compliance or defective compliance. , in the case of very serious infractions, in addition to the corresponding reputational damage.

IMPLEMENTATION

This Standard must be fully complied as of May 25, 2018, the date on which the content of the General Data Protection Regulation applies. However, the implementation of measures must begin sufficiently in advance to comply with all the provisions of the GDPR when applicable.

REVISION OF THIS STANDARD

Among the assumptions that may cause a revision of the Standard are:

- Proposals for improvement made by the audits carried out.
- Significant technological changes.

- Change in current legislation regarding what this rule expresses.

The information taken as the basis for the revision of this Standard will be communicated to the DSIGRT, who in turn will transmit it to the Information Security Steering Committee.

BREACH OF THE STANDARD

Any violation of this Standard will be sanctioned according to the disciplinary regime in force in the FCC Group, without prejudice to the provisions of the national regulations in force in each State in which the FCC Entity is located.

ADDITIONAL CONSIDERATIONS

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

The Spanish edition and the English edition will be official in centers where the language is considered official. In any other case, the English language edition will be used.

EXCEPTIONS TO THIS STANDARD

Any exception to this Standard should be justified in writing and authorized by DSIGRT.

The only way to communicate the exceptions will be the official mailbox INFOSECURITY@fcc.es and/or any other channel managed by “Service Desk FCC” to receive request.

The person responsible for the exception will be a hierarchical superior (beginning in Head of Department or C-level).

The protocol to communicate this exception will use this form:

EXCEPTIONS TO THIS STANDARD	
Applicant	
Responsible	

Policy/Code of use/Standard	
Non-compliant Section	
Description of the Exception and justification	

REFERENCES

- Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, concerning the protection of natural persons with regard to the processing of personal data and the free movement of these data and by which Directive 95/46 / EC is repealed.
- The set of Information Security guidelines of the FCC Group, from a legal, technical and organizational perspective.

DOCUMENT CHANGE CONTROL

Document Information

FILE NAME:				
VERSION	DATE	CHANGE	AUTHOR	REVIEWED BY:
1.0	February 2018	Creation of the Document	DSIGRT	Executive Security Committee
1.0	October 2019	Document Review	DSIGRT	Executive Security Committee

Las copias en papel no están controladas

FIN DEL DOCUMENTO