Privacy and Personal Data Protection Policy

PL/DIREX-PDP/019/11-22

SUMMARY

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.

1. OBJECTIVE

This policy aims to establish the general guidelines for the protection of personal data within Fundação Dom Cabral (FDC) and all its partners in Brazil and abroad. In compliance with the guidelines of this policy, the institution aims to:

- comply with the applicable laws and regulations for the protection of personal data;
- protect the rights of employees, customers, suppliers and partners against the risks of violations of personal data;
- be transparent regarding FDC's procedures in the processing of personal data;
- promote awareness throughout FDC regarding personal data protection and privacy issues.

2. SCOPE

This policy is applicable to FDC and all its partners, both in Brazil and abroad, and to all employees who have access to any personal data held by or on behalf of FDC.

Any applicable legislation in the different regions in which FDC operates must prevail, if it is or will be in conflict with this policy.

3. DEFINITIONS

For the purposes of this policy, the following are considered:

LGPD: Law No. 13709/2018, of Brazilian legislation, commonly known as the General Personal Data Protection Law (LGPD), which regulates the activities of processing personal data.

Personal Data: any information relating to an individual. For example: name; identification number; location data; online identifier; one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Sensitive Personal Data: all personal data that can generate any type of discrimination and embarrassment. Examples are: data on racial or ethnic origin; religious conviction; political opinion; membership in a union or organization of a religious, philosophical or political nature; data related to health or sexual life; genetic or biometric data.

Data Subject: any individual to whom specific, personal data refer.

Controller: those responsible for decisions regarding the processing of personal data within an institution. At FDC, the data controller is the Executive Board.

Operator: those who process personal data on behalf of the controller, including, but not limited to: employees, associated teachers and partners.

Data Protection Officer (DPO): person formally designated as the data protection officer within an institution.

Processing of Personal Data or **Processing:** any operation carried out on personal data, whether by automated or non-automated means, which include, but are not limited to: collection; registration; organization; structuring; maintenance; adaptation or alteration; retrieval; consultation; use; disclosure by

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.

transmission, dissemination or any other form of availability; comparison or interconnection; limitation; erasure or destruction.

Consent: a free, informed, and unequivocal expression by which the data holder agrees to having their Personal Data processed for a specific purpose.

Anonymization: process or technique by which personal data is rendered anonymous in such a way that it no longer renders a person directly or indirectly identifiable. Anonymity must be irreversible. Anonymized data is not considered personal data.

Pseudo-anonymization: process or technique by which the possibility of associating data directly to a person becomes more difficult (for example, mentioning of the name). The pseudo-anonymized data is still considered personal data, as it is not anonymous and it is possible, with additional information, which is kept separately, to identify the person.

Legitimate Interest: is the legal basis by which the controller may process personal data without the consent of the holder, provided that the rights and freedoms of the latter are respected and that it has justifiable processing purposes.

4. RIGHTS OF PERSONAL DATA HOLDERS

These are the rights of personal data holders, at any time and upon request:

a) To confirm whether FDC carries out processing of their personal data.
b) To have access to their data processed by FDC.
c) To be informed about how their personal data will be handled, at the time they are provided.
d) To correct their personal data if it is inaccurate, incorrect or incomplete.
e) To request deletion, blocking and/or anonymization of their personal data.
f) To oppose processing, if the processing is based on legitimate interest.
g) To withdraw consent at any time.
h) To request the portability of personal data to another service or product provider.
i) To review decisions made solely on the basis of automated processing of personal data.
j) To file a complaint with FDC, or the applicable Data Protection Authority, if they have reason to believe that any of their rights have been violated.

FDC is committed to the rights of personal data holders.

5. DATA PRIVACY COMMITTEE

The Data Privacy Committee, appointed by the Executive Board, is established.

The Committee is composed of up to six (6) members, with one employee from each of the following areas: Risk and Compliance Office, Marketing, Technology and Legal counsel. The Committee is also composed of the DPO and an invited member, the latter being optional. The duties of the Privacy Committee are defined in the section below.

6. DUTIES AND RESPONSIBILITIES[1]

6.1. The Executive Board (Controller) responsibilities:

a) Approving policies related to privacy and personal data protection.

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.

b) Approving and designating the governance structure for privacy and data protection matters, including the appointment of the Data Privacy Committee and the DPO.
c) Maintaining a record of the personal data processing operations they perform, especially when based on legitimate interest.
d) Reporting to the National Data Protection Authority (ANPD) and to the data subjects the occurrence of security incidents that may entail a relevant risk or damage to the data holders.
e) When required, prepare an impact report on the protection of personal data, including sensitive data, related to its data processing operations, as described in the legislation.

6.2. The Data Protection Officer (DPO) responsibilities:

a) Acting as a communication channel between the controller, the data holders and the ANPD, carrying out the following activities:
   I - accepting complaints and communications from holders, providing clarifications and taking action;
   II - receiving communications from the national authority and taking action;
   III - advising the entity's employees and contractors regarding the practices to be taken in relation to the protection of personal data; and
   IV - performing the other duties determined by the controller or established in the complementary regulations.
b) Acting as a consultant, together with employees, to ensure the compliance of processes involving the processing of personal data.

6.3. The Data Privacy Committee responsibilities:

a) Reviewing, when necessary, the privacy initiatives adopted by FDC, proposing improvements for the responsible areas.
b) Discussing and making technical decisions about new personal data processing activities, together with the areas proposing the respective activities.
c) Deciding on the technical measures to be applied to high-risk events.
d) Evaluating and deciding on incidents of personal data leakage, together with the data controller.

6.4. The Risk and Compliance Office responsibilities:

a) Promoting adequate knowledge of the main stakeholders regarding the importance of personal data protection and internal activities inherent to privacy initiatives.
b) Reviewing and recommending the approval of this policy and its amendments to the Executive Board.
c) Proposing the governance structure for privacy and data protection matters to the Executive Board.
d) Promoting the implementation of privacy initiatives, with the objective that FDC be in compliance with laws and regulations, as well as with its internal policies and procedures related to the subject.
e) Implementing training, awareness programs and communication on the subject to employees and third parties who work in processes related to the collection and processing of personal data.
f) Preparing, and keeping updated, the Guiding Documents related to privacy that are within its competence.
g) Conducting periodically, together with Technology Management, FDC's maturity assessments related to privacy initiatives, identifying improvements as well as their evolution.

6.5. The Legal Advisor responsibilities:

a) ensuring that contracts covering the assignment or processing of personal data contain privacy clauses appropriate to the applicable laws and regulations.
b) Providing technical support to the DPO and to the controller in the event of personal data leaks.
c) Providing technical support to FDC in the interpretation of legislation and regulations relating to the protection of personal data.

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.

d) Supporting the DPO in interfacing with National Personal Data Authorities.

6.6. The Technology Management responsibilities:

a) analyzing breaches and leaks of personal data, as well as collecting technical evidence and sharing this information with the Data Privacy Committee.
b) Implementing and monitoring security measures to ensure compliance with legislation in the processes of personal data processing.
c) Developing, and keeping up-to-date, information security policies.
d) Defining procedure for the formalization of personal data incidents.
e) Implementing mechanisms to ensure the rights of data subjects.
f) Providing technical support for the internal areas and analyzing new tools and systems focused on the protection of personal data.
g) Periodically conducting, together with the Risk and Compliance Office, FDC's maturity assessments in relation to privacy initiatives, identifying improvements as well as their evolution.
h) Providing technical support to the DPO.

6.7. Employees' responsibilities:

a) to maintain a record of the personal data processing operations they conduct, especially when based on legitimate interest.
b) To maintain the confidentiality of the personal data to which they have access in the exercise of their function.
c) Consult with the DPO before any new personal data processing activity is implemented, to ensure compliance with the legislation.
d) Act in accordance with the guidelines of this policy and of the specific legislation, taking responsibility for the appropriate processing of personal data.

7. PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA

This section describes the principles that must be observed in the collection, handling, storage, disclosure and processing of personal data by FDC.

7.1. Legality, Transparency and Non-Discrimination

FDC treats personal data fairly, transparently and in compliance with legislation, according to the legal hypotheses listed below.

a) In the execution of a contract to which the data subject is a party.
b) Requirement arising from law or regulation to which FDC is subject.
c) Legitimate interest (see definition in Item 3).
d) Provide the holder with information that allows the regular exercise of their rights.
e) To carry out studies and research - guaranteeing, whenever possible, the anonymization of personal data.
f) For academic purposes - such as registration with the Academic Department for certification.
g) For credit protection.

In cases where the processing of personal data does not fall within the above hypotheses, FDC requests the consent of the data holder, ensuring that it is provided in a specific, free, unambiguous and informed manner.

The data subject may manage and/or revoke their consent at any time, through the website: https://privacy.fdc.org.br/app/consentimento.

All collected consents are stored in such a way as to allow their verification, if requested.

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.

In some circumstances, FDC may process sensitive personal data. In these cases, more robust safety standards must be adopted.

FDC only conducts the processing of sensitive personal data, without the consent of the holder, when it is indispensable for:

a) compliance with Legal or Regulatory Obligation.
h) Regular exercise of law in contracts, judicial, administrative or arbitration proceedings.
b) Compliance with obligations and the exercise of rights in matters of employment, social security and social protection.
c) Protection of the life or physical safety of the data holder, including medical data for preventive and occupational purposes.
d) Promoting or maintaining equal opportunities among people of different racial or ethnic backgrounds.
e) Fraud prevention and guaranteeing the security of the Owner, in the processes of identification and authentication of registration in electronic systems.
f) Conducting studies and research - guaranteeing, whenever possible, the anonymization of personal data.

7.2. Limitation and Appropriateness of Purpose

FDC has a duty to process personal data in a manner compatible with the original purpose for which the data was collected, and it cannot be collected for one purpose and used for another.

7.3. Principle of Need (Data Minimization)

FDC must limit itself to collecting and processing the minimum amount of data necessary to achieve the purpose of that particular processing. That is, collecting the relevant, proportional and non-excessive data in relation to the purposes of the processing. This is the principle of data minimization.

The important thing is always to ensure that the data is relevant, within the purpose of processing, and clearly communicated to the holder.

The sharing of personal data with another area or another company must consider this principle.

7.4. Accuracy (Data Quality)

FDC must take reasonable steps to ensure that any personal data in its possession is kept accurate and up to date in relation to the purposes for which it was collected.

7.5. **Retention and Limitation of Data Storage**

FDC must know its processing activities, established retention periods, and periodic review processes. It cannot keep personal data for a period longer than necessary to meet the purposes of each processing.

7.6. Integrity and Confidentiality

FDC must ensure that appropriate technical and administrative measures are applied to personal data to protect it against unauthorized or illegal processing, as well as against accidental loss, destruction or damage. All employees with access to personal data are bound by the duties of confidentiality of personal data.

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.

7.7. Responsibility and Accountability

FDC is responsible for, and must demonstrate compliance with this policy by ensuring the implementation of various measures that include, but are not limited to:

a) ensuring that personal data holders can exercise their rights, recognized by law and by this policy.
b) Maintaining a record of the personal data processing activities it conducts and, when applicable, a record of the recipients of data sharing.
c) Maintaining a record of incidents and breaches of personal data.
d) Ensuring that third parties who are personal data operators on behalf of FDC are also acting in accordance with this policy and with applicable laws and regulations.

8. PERSONAL DATA CONTROLLER-OPERATOR RELATIONSHIP

As a rule, each FDC partner is the controller of personal data at their respective institution. In certain circumstances, the partner may act as an operator of FDC or may act as an operator of the partner, and those who are acting as an operator are obligated to follow the guidance of those who are acting as controllers.

9. DATA PROTECTION AUDITS

FDC must ensure that periodic reviews are in place to confirm that privacy initiatives, its system, measures, processes, precautions and other activities, including the management of personal data protection, are effectively implemented and maintained, and comply with applicable laws and regulations.

10. GUIDELINES

10.1. International Transfer of Personal Data

When personal data is processed in countries other than where it was collected, the legislation and regulations applicable to the international transfer of data from each country must be observed. FDC must ensure the existence and updating of contracts for international transfer of personal data.

10.2 Third-Party Service Providers

Third-party service providers who process personal data, under instructions from FDC, are subject to the obligations imposed on operators, in accordance with the applicable personal data protection legislation. FDC must ensure that privacy clauses are included in the contract for provision of service. The operator is authorized to process personal data only for the fulfillment of the contractual purpose.

10.3. Data Breach Management

All incidents and potential data breaches must be reported to the DPO. All employees must be aware of their personal responsibility to forward and to escalate potential issues, as well as to report breaches or suspected breaches of personal data, as soon as they identify them.

Data breaches include, but are not limited to: any loss, deletion, theft or unauthorized access of personal data controlled or processed by FDC.

11. GENERAL PROVISIONS

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.

It is the responsibility of the Risk and Compliance Office to clarify any doubts related to this policy, to establish the necessary procedures for its implementation, to verify and communicate the rules established in this policy.

It is the responsibility of all FDC employees and partners to comply with the guidelines established in this document.

The DPO can be contacted for the exercise of their duties at e-mail: dpo@fdc.org.br.

This document, approved on this date, revokes the Privacy and Personal Data Protection Policy PL/DIREX-PDP/012/23/08-21, of August 23, 2021, and **is expected to be revised within 2 years**.

Nova Lima, November 21, 2022.

Antonio Batista da Silva Junior
CEO

[1] In the event of the elimination of any department of FDC or external to FDC, referenced in this document, a substitution must be considered.