PERSONAL DATA PROTECTION AND PRIVACY POLICY

PL/DIREX-PDP/012/23/08-21

CONTENTS

1. OBJECTIVE

This Policy defines general guidelines for the protection of personal data in the corporate environment of Fundação Dom Cabral (FDC) and its partners in Brazil and abroad, since the conduction of its operations requires collecting, handling and storing information that may be related to identified and / or identifiable natural persons (Personal Data). With these policy guidelines, the institution aims at:

- being in conformity with applicable laws and regulations on the protection of Personal Data, and following the best practices;
- protecting the rights of collaborators, clients, suppliers and partners against the risk of violation of personal data;
- being transparent with regard to the procedures FDC adopts to handle personal data;
- promoting awareness throughout the institution regarding the protection of personal data and privacy issues.

In particular, this policy requires the institution to guarantee that the DPO (Data Protection Officer*)* is consulted before any new and significant data processing activity is launched in order to ensure that relevant conformity stages are addressed.

FDC is fully committed to ensuring the continuous and efficacious implementation of this policy and expects that all its collaborators share this commitment. Any violation of this policy may result in disciplinary action.

This policy has been approved by FDC Board Committee and Executive Board.

2. COMPREHENSIVENESS

This Policy governs **FDC** and all its **Partners**, both in Brazil and abroad, and all its **Collaborators** who have access to any personal data held by FDC or on its behalf. Additional procedures may be created to respond to requirements of local legislation.

Any legislation applicable to the different regions where FDC operates shall prevail in case it is or comes to be in conflict with this Policy.

3. REFERENCES

- FDC Bylaws
- FDC Code of Conduct
- Social Relations Covenant – FDC Code of Ethics
- European General Data Protection Regulation (GDPR)
- Brazilian General Data Protection Law (LGPD)

4. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

Anonymisation: a process or technique to make personal data anonymous in such a way that they cannot be related to any directly or indirectly identifiable person. Anonymity must be irreversible. Anonymised data are not regarded as personal data.

Collaborators: FDC employees of all levels, including executives, board members, directors, trainees and apprentices.

Data Privacy Committee: an up to five-member committee appointed by the Executive Board, including one collaborator from the Risk and Compliance Office, one from the Marketing Department, one from the Information Technology Department, one of the Legal Department and the DPO, and whose responsibilities are herein defined.

Consent: free, informed and unequivocal manifestation through which the owner agrees that his or her personal data are processed for a given purpose.

Controller: a natural or legal person, governed by public or private law, in charge of deciding matters related to the processing of personal data.

Personal Data: any information related to a singular person directly or indirectly identified or identifiable through reference to an identifier such as a name, an identification number, location data, on-line identifier or to one or more specific traits such as the physical, physiological, genetic, mental, economic, cultural or social identity of this natural person.

Sensitive Personal Data: any personal data that may result in any kind of discrimination or constraint such as, for example, data on racial or ethnic origin, religious conviction, political opinion, participation in unions or religious, philosophical or political organisations, health or sexual-life data and generic or biometric data.

Guiding Document: a formal FDC document that provides vital content related to decisions, rules and corporate guidelines to direct the course of works conducted by the institution with legitimacy, traceability and applicability. It must be observed and practiced by a defined universe of collaborators.

Data Protection Officer (DPO)*:* an individual formally appointed data protection officer, as provided in data protection legislation. The officer may be a collaborator or an outsourced resource.

Manager: any collaborator who leads a team.

Legal Department: area in charge of the management of contracts between FDC and third parties.

Legitimate Interest: the controller's legitimate interest may only substantiate the processing of personal data for legitimate purposes, concrete situations being considered, which include, but are not limited to:

- support and promotion of the controller's activities; and
- protection, with regard to the owner, of the regular exercise of his or her rights or provision of services that benefit him or her, provided that his or her legitimate expectations and fundamental rights and freedom are observed in accordance with Law number 13,709/2018.

LGPD: Brazilian federal law number 13,709/2018, commonly known as General Data Protection Law. It regulates personal data processing activities and amends articles 7th and 16th of the Brazilian Civil Rights Framework for the Internet.

Operator: a natural or legal person, governed by public or private law, in charge of processing personal data on behalf of controller, which include, but is not limited to, collaborators, associate professors and partners.

Pseudo-anonymisation: process or technique through which the possibility of associating data with other information is lessened. Data so processed cannot be directly related to identifiable persons (for instance, to

their names). Pseudo-anonymised data remain regarded as personal data because they are not anonymous, since it is possible, by processing additional information kept separately, to identify persons.

Information Technology or IT: area responsible for protecting the integrity and the confidentiality of IT systems and for implementing appropriate measures to achieve this objective. It also supports technically the DPO.

Third Party or Partner: any natural or legal person that acts in the name, on behalf or to the benefit of FDC, provides services or supply other goods, as well as commercial partners that provide services to FDC directly related to the collection, the retention or the facilitation of businesses, or deals with matters relevant to FDC, including, but not limited to, associate and guest professors, regional affiliates and other providers of professional services.

Owner of Data: individual identified or identifiable natural person to whom specific personal data refer.

Personal Data Processing or **Processing:** any operation or set of operations applied to personal data or sets of personal data by automated or non-automated means. Examples are data collection, registration, structuring, conservation, adaptation or alteration, recovery, use, disclosure by transmission, broadcasting or any other form of dissemination, comparison or interconnection, limitation, deletion or destruction.

5. ASSIGNMENTS AND RESPONSIBILITIES

5.1. The Executive Board (Controller) is in charge of:

a) approving, by the agency of its Dean, this Personal Data Protection and Privacy Policy as well as amendments to it;
b) approving the governance structure for matters of privacy and data protection, including the creation of and appointment of members to the Data Privacy Committee;
c) communicating to the national authority and to the owner any security incident that may result in relevant risk or damage to owners;
d) when required, elaborating report on the impacts on personal data protection, including sensitive data, regarding data processing operations, as provided by legislation.

5.2. Data Protection Officer (DPO) is in charge of:

a) the daily implementation of this policy;
b) acting as a communication channel between the controller, the owners of data and the Data Protection National Authority (*Autoridade Nacional de Proteção de Dados* - ANPD), conducting the following activities:
   I – reception of owners' communications and complaints, provision of information and adoption of measures;
   II – reception of communications from the national authority and adoption of measures;
   III – guidance to the entity's collaborators and employees relative to practices to be observed with regard to the protection of personal data;
   IV – completion of additional assignments given by the controller or defined by complementary norms.
c) Whenever necessary, DPO is available for the execution of his or her assignments and for obtaining additional information on this policy, via electronic mail at dpo@fdc.org.br.

5.3. The Data Privacy Committee is in charge of:

a) promoting among stakeholders the appropriate knowledge on the importance of protecting personal data and of internal activities inherent in privacy initiatives;

b) reviewing, whenever necessary, the privacy measures adopted by FDC and recommending improvements to applicable areas;
c) discussing and making technical decisions on new activities involving processing of personal data, in conjunction with the areas proposing said new activities;
d) deciding on technical measures to the adopted in case of high-risk events and on disciplinary measures, whenever necessary;
e) evaluating and deciding on personal data leak incidents, in conjunction with the Executive Board.

5.4. The Risk and Compliance Office is in charge of:

a) reviewing and recommending approval of this policy and its amendments to the Executive Board;
b) proposing a governance structure for matters of privacy and data protection to the Executive Board;
c) permanently and effectively monitoring the implementation of privacy initiatives in order to comply with laws and regulations on personal data protection and privacy, as well as with related internal policies and procedures;
d) implementing training, communication and awareness programmes on the subject personal data privacy to be offered to collaborators and outsourced personnel working in processes related to the collection and processing of personal data;
e) elaborating and updating Guiding Documents related to privacy and within its competence;
f) supporting the elaboration and the update of privacy notices;
g) periodically conducting evaluations of FDC maturity regarding privacy initiatives, identifying improvements and evolution.

5.5. The Legal Department is in charge of:

a) making sure that contracts involving personal data cession or processing include privacy provisions in compliance with applicable legislation and regulations;
b) providing legal support to the DPO, to the Data Privacy Committee and to the Executive Board in case of personal data leakage;
c) providing legal support to FDC regarding the interpretation of legislation and regulations on the protection of personal data;
d) supporting the renegotiation of contracts and / or amendments with suppliers and partners that conduct personal data processing;
e) supporting the DPO in contacts with Personal Data National Authorities.

5.6. The Information Technology Department is in charge of:

a) investigating violations and leakages of personal data as well as collecting technical evidences and sharing information with the Data Privacy Committee;
b) monitoring ad implementing security measures for guaranteeing compliance with applicable legislation and regulations;
c) publishing privacy notices in websites and external programmes;
d) revising and updating the Guiding Documents within its competence with respect to information security;
e) defining procedures and templates for official report of personal data incidents;
f) implementing mechanisms for guaranteeing the rights of data owners;
g) providing technical support to internal areas and analysing new systems and tools, focusing on exposure of personal data;
h) guaranteeing the application of technological security measures proportional to the risk inherent in personal data processing and aligned with the security expectations of data owners, ensuring integrity, availability and confidentiality of information.

5.7. All Collaborators shall:

a) appropriately handle personal data and act according to the guidelines of this Policy;

b) before implementing new personal data processing activities, submit corresponding proposals to the analysis of the Data Privacy Committee.

6. GUIDELINES

6.1. Personal Data Protection Principles

This sections describes principles to be upheld when collecting, handling, storing, publishing and processing personal data at FDC, so as to meet corporate data protection standards and comply with applicable legislation and regulations of countries where it maintains operations or educational activities.

6.1.1. Legality, Transparency and Non-discrimination

FDC processes Personal Data in a fair and transparent way and in compliance with applicable legislation and regulations.

FDC only processes personal data when the purpose or objective meets the requirements of the allowed legal hypotheses listed below:

a) when processing is required to execute a contract of which owner of data is a party;
b) when processing is required by law or regulation to which FDC is submitted;
c) when in legitimate interest, as defined by item 4 of this Policy;
d) when processing is required to enable owner of data to regularly claim data owner's rights in judicial, administrative or arbitral procedures;
e) when processing is required to conduct studies and researches, ensuring, whenever possible, the anonymisation of personal data;
f) when processing is required for academic purposes, for instance when registering for certification at the Academic Department;
g) when processing is required to protect credit, including provisions by pertinent legislation.

When the desired processing of personal data does not match the hypotheses above, FDC shall obtain consent from owner of data to process owner of data's personal data, and make sure said consent be obtained in a specific, free, unequivocal and well-informed manner. FDC shall collect, store and manage all consents in an organised and accessible way, so that proof of consent may be supplied whenever necessary.

Consent may also be provided by the owner of data when filling application forms and templates in FDC websites and applications - or electronically by owner of data - when the purposes of the processing are explicitly identified and may include promotion of FDC educational programmes and institutional messages.

Similarly, the owner of data is responsible for withdrawing owner of data's consent at any time, as easily as when giving it.

Processing of sensitive personal data is allowed only in the specific situations described below, and such processing shall comply with higher security standards as those adopted when processing other personal data:

a) when processing is required to comply with legislation or regulations;
b) when processing is required to regularly claim rights in judicial, administrative or arbitral procedures;
c) when processing is required to fulfil obligations and exercise rights in matters related to employment, social security and social protection;
d) when processing is required for the protection of life or physical integrity of owner of data, including medical data for occupational or preventive purposes;

e) when processing is required to promote or maintain equal opportunities for people of different racial or ethnic origin;
f) when owner of data gives explicit consent, in accordance with applicable legislation and regulations;
g) when processing is related to penal convictions, violations or protective measures, processing shall be carried out under the control of the public authority, or when processing is authorised by Federal or State legislation which includes appropriate safeguards for the rights and freedom of owners of personal data.

In some circumstances, FDC may have to process sensitive personal data involving, but not limited to:
a) data related to health or the sexual life;
b) genetic or biometrical data linked to a natural person;
c) data on sexual orientation;
d) data on convictions or criminal offences;
e) data related to racial or ethnical origin, religious beliefs, political opinion, membership in union or in religious, philosophical or political character organisation.

6.1.2. Limitation and Adequacy of Purpose

Processing of personal data must be conducted in a compatible way with the original purpose for which personal data were collected; they may not be collected for one purpose and used for another purpose.

6.1.3. Need-to-know Principle (Minimisation of Data)

FDC may only process personal data to the extent that it is necessary to achieve a specific purpose; this is the minimisation of data principle. Sharing of personal data with other areas or other companies shall take this principle into consideration, and data may only be shared when appropriately allowed by law.

6.1.4. Accuracy (Quality of Data)

FDC shall take reasonable measures to ensure that any personal data it holds are kept accurate and update relative to the purposes for which they have been collected, and owners of personal data must offered the possibility of demanding exclusion or correction of inaccurate or out-dated data.

6.1.5. Retention and Limitation on Data Storage

FDC must be aware of its processing activities, established retention periods and periodical revision processes, and FDC shall not keep personal data for a period longer than the necessary to achieve the intended purposes.

6.1.6. Integrity and Confidentiality (Free Access, Prevention and Security)

FDC shall make sure that appropriate technical and administrative techniques are applied to personal data so as to protect them against unauthorised or illegal processing, as well as against accidental loss, destruction or damage. Processing of personal data must also provide the necessary confidentiality. Among the most common technical measures we may mention anonymisation and pseudo-anonymisation, as defined in item 4 of this Policy.

6.1.7. Accountability and Submission of Accounts

FDC is responsible for and must demonstrate the enforcement of this policy, making sure that several measures are taken, including, but not limited to:

a) the guarantee that owners of personal data may exercise their rights as provided by legislation and this policy;
b) registration of personal data, including:
   - register of personal data processing activities, including description of the purposes or objectives of said processing, of those entitled to share personal data and of periods during which FDC may retain them;
   - register of personal data incidents and personal data violations.
c) the guarantee that third parties that are Personal Data Operators are also acting in accordance with this Policy and with the applicable legislation and regulations;
d) the guarantee that FDC, when required, register a Data Protection Officer (DPO) at National Authority;
e) the guarantee that FDC complies with all requirements and requests of any supervising authority to which it is subject.

6.2. Security Standards

6.2.1. Importance of Protecting Personal Data

FDC is committed to the implementation of information security standards and to the protection of personal data in order to guarantee the individual's fundamental right to self-determination regarding information.

6.2.2. Guarantee of Personal Data Security

Confidentiality, integrity and availability, as well as authenticity, accountability and non-repudiation, are objectives to be pursued to achieve personal data security.

6.2.3. Obligation of Personal Data Confidentiality

All collaborators who have access to personal data are automatically submitted to the duty of confidentiality of personal data in that they agree with FDC's Code of Conduct and Code of Ethics, by the time they are admitted as employees by the institution and periodically, as necessary.

6.2.4. Privacy of Personal Data from Conception and by Default

When implementing new processes, procedures or systems that involve personal data, FDC shall adopt measures to guarantee that privacy and data protection rules are applied since the very beginning of conception up to the launching or implementation of said projects.

6.3. Relationship between Personal Data Controller and Operator

As a rule, each FDC partner is a Personal Data Controller within the respective organisation, and a responsible person must be appointed to guarantee that personal data are being correctly processed and in accordance with applicable laws and regulations. In certain circumstances, a partner may act as partner's Operator and, in this case, the Operator shall follow the guidelines provided by the party that is acting as Controller.

6.4. Personal Data International Transfer Policy

When personal data are processed in countries different from where they were collected, each country's regulations and legislation applicable to the international transfer of data must be complied with. FDC shall ensure the existence and regular update of contracts addressing the international transfer of personal data.

6.5. Rights of Owners of Personal Data

FDC is committed to the rights of owners of personal data, which include:

a) right to information on how personal data will be handled, to be provided when personal data are submitted;
b) right to information on the processing of Owner's personal data, as well as the right to access Owner's personal data stored by FDC;
c) right to corrections to personal data when not precise, incorrect or incomplete;
d) right to the exclusion, blocking and / or anonymisation of Owner's personal data in certain circumstances (the "right to be left alone").This may include, but does not limit to, these circumstance when there is no need for FDC to retain Owner's personal data for the purposes they have been collected for;
e) right, under certain conditions, to restrict processing of Owner's personal data;
f) right to oppose processing, when processing is based on legitimate interest;
g) right, at any moment, to withdraw consent, if processing of personal data is based on individual consent and for a specific purpose;
h) right to portability of personal data and to transfer them to other service or product provider by means of explicit requisition, under certain circumstances;
i) right to the review of decisions based exclusively on automated processing of personal data;
j) right to submit complaints to FDC or to the pertinent Data Protection Authority, if Owner of Personal Data has reason to suppose any of Owner's rights to the protection of personal data has been violated.

6.6. Third-party Service Providers

Third-party service providers that process personal data under FDC supervision are subject to obligations imposed on Operators according to applicable personal data protection legislation and regulations. FDC shall make sure that the service provision contract includes privacy clauses that require third-party data Operators to implement security measures and appropriate technical and administrative controls to ensure confidentiality and security of personal data, and to establish that Operator is only authorised to process personal data when such processing is formally requested by FDC.

In cases when service provider operates outside the country where personal data has been collected, standard contractual clauses must be included in the personal data protection contract as appendix, to guarantee that safeguards required by applicable personal data protection legislation and regulations are implemented.

6.7. Management of Data Violations

Every incident and potential violation of data must be reported to the Data Protection Officer - DPO. All collaborators must be aware of their personal responsibility for forwarding and scaling potential problems as well as for denouncing Personal Data violations or suspected violations as soon as they come to their knowledge. When an actual incident or violation is found, it is essential that the incidents are formally and tempestivily reported.

Data violations include, but are not limited to, any loss, exclusion, theft or unauthorised access to personal data controlled or processed by FDC.

6.8. Data Protection Audits

FDC shall guarantee that periodical revisions are conducted, in order 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 legislation and regulations.

7. GENERAL PROVISIONS

The collaborators are obliged to get acquainted with and understand all applicable Guiding Documents. Similarly, managers are responsible for ensuring that all collaborators in their teams understand and follow the provisions of Guiding Documents applicable to FDC.

Violations against any Guiding Document, including against this Policy, may result in serious consequences to the institution and to involved collaborators. Therefore, failure to pursue this Policy or to report a violation of this Policy may result in person being held liable, according to FDC internal policies and / or to applicable legislation.

Collaborators who have any doubts or questions about this Policy, including its scope, terms or obligations, must refer to their respective managers and, if necessary, to the DPO or to FDC Risk and Compliance Office.

This Policy is in effect as of the date hereof and revokes all previous provisions.

Nova Lima, August 23, 2021.

Antonio Batista da Silva Junior
Dean

Next Revision: in up to 2 years from the date hereof.