PRIVACY AND PERSONAL DATA PROTECTION POLICY

MARCH 2022

DCI – INTERNAL CONTROL DIVISION

SUMMARY

1. CONTEXTUALIZATION 3
2. RECIPIENTS 3
3. APPLICABILITY 3
4. OBJECTIVES 3
5. MAIN ELEMENTS OF LGPD 3
5.1. Principles of LGPD 4
5.2. Lawful basis of LGPD and attention to data of children and adolescents 4
5.3. International data transfers in LGPD 5
6. DUTIES AND RIGHTS RELATED TO PERSONAL DATA 6
6.1. Duties 6
6.2. Rights 6
7. LGPD COMPLIANCE PROGRAM 7
7.1. Team responsible for the LGPD Compliance Program at FGV 7
7.2. Maximum Instance for Issues Related to Information Security at FGV 7
7.3. Compliance with Personal Data Protection in relationships with third parties 7
7.4. Training, Monitoring and Updates 8
SINGLE APPENDIX – GLOSSARY 9

1. CONTEXTUALIZATION

This *Privacy and Personal Data Protection Policy** ("*Policy*") aims to provide guidance on the various **personal data**[1] **processing** activities carried out by Fundação Getulio Vargas – **FGV**.

This document is part of a compliance program developed and executed by **FGV** to comply with the **Brazilian General Data Protection Law** (Law no. 13.709/2018 – "**LGPD**") and other sectoral laws on the subject. This program started in May 2019, integrating the strategic actions of the **FGV Internal Controls and Compliance System**, coordinated by the **Internal Control Division (DCI)**.

2. RECIPIENTS

This *Policy* is applicable to (i) **FGV** employees; (ii) authorized **third parties** acting on behalf of **FGV** in the **processing of personal data**; (iii) external **personal data processing entities** (either legal entities or natural persons) which are somehow related to the organization; and (iv) **data subjects** (natural persons) whose data are **processed** (used in a broad sense) by **FGV**.

3. APPLICABILITY

This *Policy* establishes guidelines and rules so that its recipients understand and, according with their respective roles, comply with the provisions contained in the applicable legislation that deals with the protection of **personal data** (whether they are in any format, printed or electronic) within the scope of the activities provided for in the **FGV** Statute.

4. OBJECTIVES

These are the objectives of this *Policy*, which must be read and interpreted alongside with the other internal Rules, Ordinances, legal instruments and other **FGV** guidelines on the subject.

- Describe, without pretense of exhaustion, the main guidelines and obligations for the protection of **personal data** of the **LGPD** to the recipients of this *Policy*;
- Introduce the main Teams responsible for carrying out **LGPD** compliance actions at **FGV** and the internal channels for questions and general communications.

5. MAIN ELEMENTS OF LGPD

[1] The words highlighted in bold format in this document are defined in the *Glossary*, presented in the Single Appendix.

5.1. Principles of LGPD

Principles are "compasses" that aid in the interpretation of a legal provision in certain cases. **LGPD** has a set of principles[2], among which stand out, without prejudice to the others, those of *necessity*, *security*, and *accountability*.

Necessity infers that it shall be analyzed which **personal data** are effectively needed in order to achieve a certain purpose among all those that could be used in an operation. Thus, it shall be avoided the collection of more **personal data** than those effectively needed to meet that specific end. *Security* provides that good administrative and technological practices must be implemented to protect **personal data**. The occasional compromise or misuse of these data shall be accurately assessed. The principle of *accountability* points to the necessity of seeking methods for improving processes and routines in the organizations, apart from the promptitude to demonstrate the actions taken to comply with **LGPD** to the Public Authorities and to the **data subjects**.

5.2. Lawful basis of LGPD and attention to data of children and adolescents

Besides the principles that aid the comprehension of the guidelines of **LGPD**, this Law also brings the concept of lawful basis which is, in short, a prerogative for organizations to **process personal data** in specific situations.

The Law establishes different rules to regulate the **processing of personal data** and **sensitive personal data**[3] (special categories of **personal data**). Observed the lawful basis of **LGPD**, **FGV** mostly uses the ones listed below, without prejudice to others not included.

---

[2] Art. 6° The activities of processing of personal data shall observe good faith and the following principles:
I- purpose: carrying out the processing operation for legitimate, specific, explicit and informed purposes to the data subject, without the possibility of further processing in a way that is incompatible with these purposes;
II- adequacy: compatibility of the processing operation with the purposes informed to the data subject, according to the context of the processing operation;
III- necessity: limitation of the processing operation to the minimum necessary for the accomplishment of its purposes, including the relevant, proportional and not excessive data in relation to the purposes of the data processing;
IV- free access: guarantee, to the data subjects, of facilitated and free consultation on the form and duration of the processing, as well as on the completeness of their personal data;
V- data quality: guarantee, to the data subjects, of accuracy, clarity, relevance and updating of the data, according to the need and for the fulfillment of the purpose of its processing;
VI- transparency: guarantee, to the data subjects, of clear, precise and easily accessible information about the execution of the processing and the respective processing entities, observing the commercial and industrial secrets;
VII- security: use of technical and administrative measures capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication or dissemination;
VIII- prevention: adoption of measures to prevent the occurrence of damages due to the processing of personal data;
IX- non-discrimination: impossibility of carrying out the processing operation for illicit or abusive discriminatory purposes;
X- accountability: demonstration, by the data processing entity, of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures.

- To comply with legal or regulatory obligations, such as guidelines, ordinances, or regulation for using and maintaining the data issued by the Ministry of Education;
- During research activities of its Centers and Units to develop studies;
- When necessary to the regular exercise of rights, whether regarding contracts or legal, administrative and arbitration procedures;
- For the protection of life and physical safety of a natural person or for health protection alongside with healthcare professionals and services;
- When it aims to prevent frauds or to protect people's safety in case of identification and authentication of their electronic systems;
- After obtaining the consent of the person to whom these data refer;
- Aiming to comply with contracts or procedures related to contracts in general, from which the person whose data are **processed** benefits as an example of academic service contracts and the obligations arising therefrom;
- When it is needed to attend to legitimate interests, respecting the limits provided by **LGPD**;
- For credit protection.

Of the hypotheses above, the last three ones – which are underlined – represent situations foreseen solely for **processing personal data**, which differs from the others that can justify the use of **sensitive data** and/or **personal data** on a case by case basis.

Lastly, it is necessary to highlight operations which involve **personal data** of adolescents (in Brazil, known as those between 12 and 17 years old) and children (in Brazil, known as those between 0 and 11 years old). **LGPD** stated special conditions for its **processing**, especially when it comes to children since as a rule it is necessary to obtain the authorization of one of their parents or legal guardian in order to use their data in certain operations.

5.3. International data transfers in LGPD

International data transfers of **personal data** means, in **LGPD**'s scope, the sharing of **personal data** with organizations or people located in other countries besides Brazil.

To develop its regular activities, **FGV** may need to transfer **personal data** to entities located in other countries, mainly for performance of contracts that regulate academic exchanges or offering platforms from **Suppliers** whose technological infrastructure is not restricted to Brazil.

In those cases, **FGV** shall observe the specific provisions of **LGPD** and the norms published by the **Brazilian National Personal Data Protection Authority** (acronym "**ANPD**"), as mentioned

[3] Sensitive personal data: personal data on racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sex life, genetic or biometric data, when linked to a natural person. At FGV, financial data (see glossary after the Policy) may be considered sensitive in relation to its conservation method.

in the Privacy Notice, Terms of Use, Contracts and, whenever requested, Authorization and/or Consent Terms.

6. DUTIES AND RIGHTS RELATED TO PERSONAL DATA

6.1. Duties

The duties of proper usage of **personal data** (or of systems that may contain them) apply to all the recipients of this *Policy* according with their roles at **FGV**.

When the recipient of this *Policy* is an employee, a scholarship student, a self-employed or a **Third-party**'s service provider that performs operations using **personal data**, it is essential to observe the principle of *necessity*, thus **processing** only strictly necessary data and within the purposes of the regular activities developed, as well as the principle of *security*, maintaining the secrecy over the information accessed thus not revealing or exposing them to unauthorized entities. It is also an obligation to contact the official channels dpo@fgv.br or comitedeseguranca@fgv.br in case of detecting suspicious situations or in the presence of doubts, suggestions, or complaints regarding this theme.

When the recipient of this *Policy* is a **data subject** who had his/her **personal data processed** in an operation of **FGV**, he/she compromises to cooperate and observe the instructions on the Contracts, Terms of Use or guidance received, thus not sharing credentials with unauthorized entities, and to keep devices protected. In case of doubts, complaints, or suggestions, it is necessary to contact the channels mentioned in the paragraph above.

6.2. Rights

All **data subjects** have guaranteed[4] the rights granted by **LGPD** when their **personal data** are **processed** by an organization.

[4] Art.18. The data subject, regarding the data subject's data being processed by the controller, at any time and by means of request, has the right to obtain the following from the controller:
I- confirmation of existence of a processing operation;
II- access to data;
III- correction of incomplete, inaccurate or outdated data.
IV- anonymization, blocking or erasure of unnecessary, excessive or irregular processed data in violation of the provisions of this Law;
V- data portability to another service or product provider, upon express request, in accordance with the regulation of the national authority, observing commercial and industrial secrets;
VI- erasure of personal data processed with the consent of the data subject, except in the cases provided for in article 16 of this Law;
VII- information about public and private entities with which the controller made shared use of data;
VIII- information about the possibility of not providing consent and about the consequences of such denial;
IX- revocation of consent, pursuant to paragraph 5 of article 8 of this Law.
§1°- The personal data subject has the right to petition in relation to his/her data against the controller before the national authority.
§2°- The data subject may object to processing operation that is carried out based on one of the hypotheses of exemption of consent, in the event of non-compliance with the provisions of this Law.

Regarding **FGV**, the official channel for the exercise of the rights guaranteed by **LGPD** is available at the following address: https://portal.fgv.br/en/personal-data-protection, by clicking and registering the option "Check out our Privacy Central". The **personal data subjects** who are unfamiliar with Portuguese language can, exceptionally, request these rights through the e-mail: dpo@fgv.br.

In case the **data subject** uses any of **FGV** systems in which he/she has a login and a user's profile, it is possible to use the options for correcting information directly offered in these systems (*e.g.,* update **personal data**). The e-mail and the address previously indicated are offered as complementary channels.

7. LGPD COMPLIANCE PROGRAM

7.1. Team responsible for the LGPD Compliance Program at FGV

LGPD establishes a legal character to concentrate actions of compliance in the organizations, the **Data Protection Officer** ("**DPO**"). It is **FGV**'s **DPO** prerogative, through **DCI**, to conduct the LGPD Compliance Program, intermediating the relation between its **Units**, further institutions, the **Data Subjects,** and Public Authorities.

The **DPO** can be contacted via e-mail (dpo@fgv.br) by anyone in case of doubts, suggestions, complaints, or communications related to **personal data** as well as for situations not provided in this *Policy*.

7.2. Maximum Instance for Issues Related to Information Security at FGV

In its structure, **FGV** counts on its Information Security Committee, without prejudice to pertinent Teams, Direction Boards and Superintendencies. This Committee is the maximum instance foreseen in **FGV**'s *Information Security Policy* for decisions regarding assets of information and **personal data**.

In case of suspicions or confirmations of violations as well as notifications of vulnerabilities involving **FGV**'s systems or records shall be communicated directly to the Information Security Committee via e-mail comitedeseguranca@fgv.br.

7.3. Compliance with Personal Data Protection in relationships with third parties

It is **DCI**'s prerogative to conduct the LGPD Compliance Program according to the guidance provided by **FGV**'s **DPO** to assess risks in the contractual and non-contractual relationships. In this sense, observed the internal norms concerning this theme, **FGV** can request to the related

Art. 20 The data subject has the right to request the review of decisions solely based on automated processing of personal data that affect his/her interests, including decisions aimed at defining personal, professional, consumer and credit profile or aspects of his/her personality.

third-parties the filling of questionnaires, testimonies, and the exhibition of evidences regarding compliance with **LGPD**.

7.4. Training, Monitoring and Updates

The recipients of this *Policy* shall take part in the trainings and other actions promoted by **FGV** whenever requested and observed their respective roles, fulfill this *Policy* and cooperate with the **personal data** protection culture.

FGV shall keep the continuous monitoring and the improvement of its compliance actions as it can also review the current *Policy* periodically, publishing its new version.

Document	Privacy and Personal Data Protection Policy
Dimension	Normative Structure of Procedures
Type of Normative Instrument	Policy
Subject Category	Control and Compliance
Subject	Compliance System
ID	CC.01.003.2022
Previous Version	1.0/2020 (CC.01.001.2020)

ELABORATION	APPROVAL
Name: Jordan Vinícius de Oliveira	**Name:** Carlos Ivan Simonsen Leal
Position: Data Protection Officer	**Position:** President
Version: 2.0/2022	**Ordinance Nº**: 17/2022, de 30/03/2022

***Note:** small adaptations were made in the translation of the Portuguese to English version.

SINGLE APPENDIX – GLOSSARY

BRAZILIAN GENERAL DATA PROTECTION LAW ("LGPD"): Law no. 13.709/2018, General Data Protection Law that regulates the **processing of personal data** in digital or physical media when performed by a natural person or legal entity under public or private law.

BUSINESS PARTNERS: At **FGV**, the **business partners** shall be considered as the **third-parties** contracted, either as natural person or legal person, who perform in the institution's name, such as Consultants, Partner Educational Institutions and Commercial Agents.

DATA PROTECTION OFFICER ("DPO"): At **FGV**, person from its **Internal Control Division** (**DCI**) nominated by the Presidency, according to Internal Ordinance 67/2020, to maintain and monitor its compliance program to **LGPD** and applicable legislations.

DATA SUBJECT: Natural person to whom the **personal data processing** operations refer.

FGV'S INTERNAL CONTROL AND COMPLIANCE SYSTEM (SCIFGV): Formed by an integrated and dynamic set of elements that helps the Institution to achieve its strategic objectives, as well as its mission, vision and values, guiding its development and reasonably guaranteeing its efficiency and effectiveness management of risks in order to ensure its sustainability and growth.

FGV UNITS: Internal areas that comprise the following structure: Senior Management; General Administration; Services, Indexes and Publications; Education and Research; and Special Programs.

FINANCIAL DATA: Regarding the objectives of this *Policy*, they are related to the economic life of a natural person. For the purposes of equal maintenance conceived to **sensitive personal data**, **financial data** are understood as those that may cause harm or relevant risk to **data subjects** in the occurrence of an adverse event.

NATIONAL DATA PROTECTION AUTHORITY ("ANPD"): Public Administration body that is responsible for ensuring, implementing and supervising the application of **LGPD** whenever applicable, guarded its technical autonomy.

PERSONAL DATA: Data linked to an identified or identifiable natural person.

PROCESSING ENTITIES: Entities responsible for **processing personal data** classified as **Controller** (who decides) or **Processor** (who follows the orders given) of the **processing**.

PROCESSING OF PERSONAL DATA ("PROCESSING"): Any operation carried out with **personal data** such as: collection, production, receipt, classification, use, access, reproduction, transmission, distribution, **processing**, storage, filing, erasure, evaluation or information control, modification, communication, transferring, dissemination or extraction.

SENSITIVE PERSONAL DATA: **Personal data** concerning racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sex life, genetic or biometric data, when linked to a natural person.

SUPPLIERS: Other contracted or subcontracted **third-parties**, whether natural persons or legal entities, not defined as **business partners**.

THIRD PARTY: **Business partners** and/or **suppliers** related to **FGV**.

DICOM