

APPLICANT PRIVACY STATEMENT

1. PURPOSE

This Applicant Privacy Statement ("Privacy Statement") discloses detailed information on the different types of Data from applicants that Itaúsa S.A. ("Itaúsa" or "Company") can collect or store in the course of a selection process for employment, internship or apprenticeship, how Itaúsa can use this Data, as well as why it collects and uses it, among other information related to this Data Handling.

2. RESPONSIBILITIES AND TARGET AUDIENCE

Itaúsa is responsible for Handling the Personal Data it collects or otherwise uses, acting as your potential future employer and selection process manager. Under Applicable Data Protection Laws, Itaúsa is the Data Controller.

This Privacy Statement is intended for all applicants who apply for and/or participate in a selection process for employment, internship or apprenticeship at Itaúsa.

3. WHAT ARE THE PRINCIPLES UNDERLYING OUR HANDLING OF YOUR DATA?

Itaúsa is driven at all times by the ten principles set by the Applicable Personal Data Protection Laws, as follows: purpose, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination, and accountability.

4. WHICH DATA FROM APPLICANTS DO WE COLLECT AND HOW WE USE IT?

- We can collect or receive Data directly from applicants through:
 - our e-mail,
 - our website,
 - LinkedIn,
 - Interviews conducted.
- We can also receive Data from third-party recruitment agencies that are partners to Itaúsa.

Some of the Data we request is **mandatory** for the reasons below:

- to respond to a request sent by the applicant (e.g., to confirm the application for an open position, to send information about the progress of the application process, etc.);
- to evaluate the application for an open position at Itaúsa; and
- to fulfill our legal obligations (e.g., concerning labor legislation).

The non-provision of requested mandatory information may impact our evaluation of the application or the outcome of recruitment processes.

- **Sensitive Personal Data**

In some cases, Itaúsa will need to handle Sensitive Personal Data. This will require higher data protection levels, which will be considered whenever the need arises, at all times for specific purposes and to the extent required accordingly.

- **Parties with which we share your Data**

Your Personal Data can be shared with service providers whenever required to meet the purposes of the selection process and on a need-to-know basis only. We will always endeavor our best efforts to ensure that all third parties we work with will safeguard your Personal Data.

Furthermore, we can share your Personal Data whenever required by law or due to any administrative, arbitration ruling or judicial order.

Sometimes Itaúsa may need to transfer your Personal Data outside of Brazil (e.g., if a Data storage server is located elsewhere). We will only do so in a safe way and according to the law, requiring that recipients of this Data comply with all commitments set in this Privacy Statement.

- **For which purposes we use your Personal Data**

Your Personal Data is solely used in the course of the process selection.

- **Legal grounds for handling your Personal Data**

- By consent
- On the grounds of Itaúsa’s lawful interest
- To formalize an employment, internship or apprenticeship contract
- To meet any legal or regulatory obligations or for the regular exercise of rights under a judicial, administrative or arbitration proceeding
- To prevent frauds and ensure the security of your Data in processes of identification and authentication of registers at electronic systems

TABLE: HANDLING OF PERSONAL DATA

Contexts in which your Data can be handled	Data that can be handled	With whom your Data may be shared	Purposes of our use of your Personal Data.
Application for an open position; Recruitment, interviews and evaluation process; Procedures before signing a contract. By email, LinkedIn, in-person delivery of résumés or through recruitment agencies	<ul style="list-style-type: none"> • Identifiers (e.g.: Name, surname, profession). • Identifiable documents (e.g.: Identity card (RG), Individual Taxpayer’s Registry (CPF). • Contact information (e.g., email, phone number, address). • Information about dependents (e.g., name, age). • Professional background (e.g.: previous professional experiences, referrals). • Education (e.g., education background, language proficiency). • Sensitive Personal Data (on health, racial or ethnic origin, and biometry) • Photo 	Recruitment agencies and data storage service providers	<ul style="list-style-type: none"> • Getting to know you • Evaluating capacities in the recruitment scope • Organizing and conducting recruitment and interview processes • Designing the employment contract • Organizing your onboarding at Itaúsa

5. HOW LONG WILL WE RETAIN YOUR PERSONAL INFORMATION?

Your Personal Data handled by Itaúsa may be stored throughout the application process and up to five (5) years from the decision to refrain from hiring you, except if longer storage terms are required under the Applicable Data Protection Laws or to meet any legal obligation or preserve the Data Subjects’ regular rights. If you are hired, the Handling of your Personal Data will be governed by our Employee Privacy Statement.

When Itaúsa no longer needs to use your Personal Data for the purposes listed above, such data will either be safely removed from all systems in which it is stored or anonymized in a way that you will no longer be identifiable based on such data.

6. WHAT MEASURES ARE ADOPTED FOR DATA SECURITY PURPOSES?

Itaúsa adopts technical means and security procedures suitable to protect Personal Data from any undue use, unauthorized access, interference, change, disclosure or loss in order to conform with the confidentiality and inviolability of Personal Data.

7. HANDLING CHILDREN'S DATA

Itaúsa will only handle personal data from minors under 12 years of age if they are dependents, and solely in the case this information is relevant to Itaúsa's selection process. We underscore that we will request the express specific consent from the applicant legally responsible for the minor.

8. WHAT ARE YOUR RIGHTS?

Under Applicable Data Protection Laws, you have the following rights concerning Personal Data:

- **Confirming the existence of Data Handling**

You have the right to ask us whether we will handle Personal Data.

- **Receiving information**

You have the right to receive information on the public or private entities with which we will share Personal Data and receive information on our Handling of this Personal Data.

- **Accessing Data**

You have the right to access your Personal Data that is held by us, as well as in some cases to receive an electronic copy of this Data, according to the Applicable Data Protection Laws.

- **Correcting Data**

You have the right to rectify Personal Data that is inaccurate, incomplete or outdated.

- **Deleting Consent Data**

You have the right to request your Consent Data to be excluded from our databases, except in the case we are legally supported to proceed with the Data Handling, for example, the need to comply with any legal obligation.

- **Requesting Personal Data Anonymization**

You have the right to request Anonymization, which is the process of encrypting or removing Personal Data construed as unnecessary or excessive or Personal Data not being Handled in conformity with the Applicable Data Protection Laws.

- **Revoking consent**

You have the right to revoke the consent for Handling Personal Data at any time in the case of Consent Data. You also have the right to be informed of the possibility of not providing consent and the consequences of such refusal. If applicable, we will cease the Data Handling except if we are legally supported to proceed accordingly.

- **Motion**

You have the right to file a motion with the National Data Protection Authority (ANPD) against Itaúsa's Data protection and privacy practices. However, we hope you feel comfortable enough to contact us before

submitting any formal complaint to the proper authorities. We are at your disposal to provide help and answer any questions you may have.

9. CHANGES TO THIS STATEMENT

This Statement may be revised from time to time. If any material changes are made, we will disclose a new version hereof on the Website, under Applicable Data Protection Laws. If any change requires your consent, we will request you to provide it accordingly. We encourage you to review this Statement from time to time to keep up to date on our Data Handling practices.

10. CONTACT INFORMATION

If you have any questions about this Privacy Statement, please contact our Data Protection Officer (DPO), Ms. Maria Fernanda Caramuru, via email dadosprotegidos@itausa.com.br accessible on the bottom bar of our website homepage.

11. GLOSSARY

Capitalized terms, as defined below, used in this Statement will have the meanings as follows. Any other capitalized terms, even if not defined in this Glossary, must be construed according to the Applicable Data Protection Laws.

- "Personal Data" or "Data": any information related to an identified or identifiable natural person.
- "Sensitive Personal Data" or "Sensitive Data": Personal Data on racial or ethnic origin, religious belief, political opinion, association to a workers' union or a religious, philosophical or political organization, data related to health or sexual life, genetic or biometric data.
- "Anonymization" or "Anonymized": adoption or reasonable, available technical means during Data Handling, through which a piece of data loses the possibility of being directly or indirectly associated with an individual.
- "Handling" or "Handle" or "Handled": any and all operations carried out by using Personal Data, such as those related to information collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control, change, communication, transfer, disclosure or extraction.
- "Applicable Data Protection Laws": Brazilian General Personal Data Protection Act No. 13709/2018 ("LGPD"), as amended, as well as the Brazilian Civil Rights Framework for the Internet No. 12965/2014, Decree No. 8771/2016, Brazilian Federal Constitution, Brazilian Civil Code, Brazilian Penal Code, Brazilian Consumer Protection Code Decree No. 7963/2013, and any other laws and regulations related to the Handling of Personal Data and privacy applicable to a party and, if applicable, all guidelines and codes of practices issued by the National Data Protection Authority ("ANPD") or other proper Data protection or surveillance authorities.