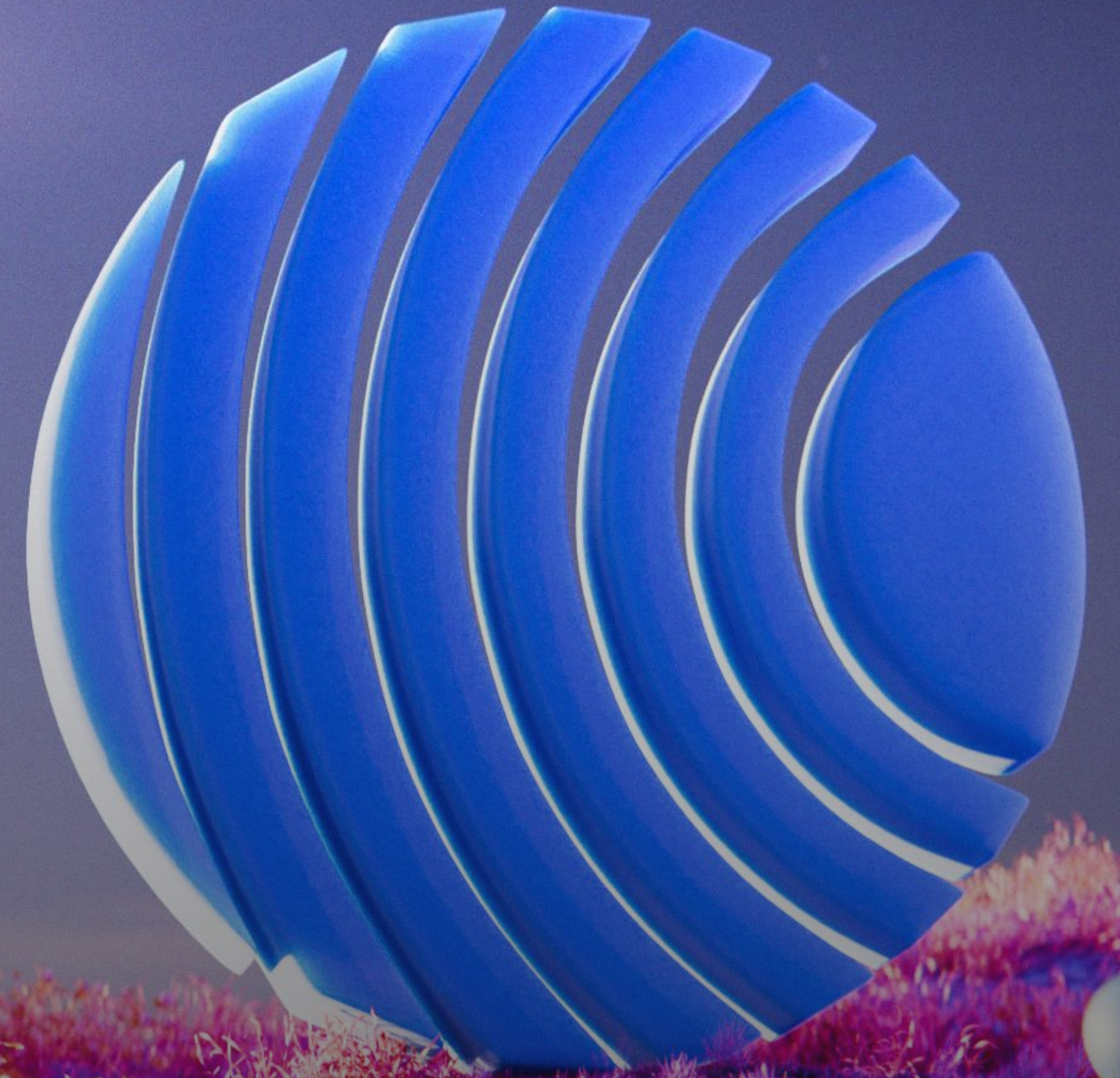




Privacy Notice for CloudWalk Candidates



Summary

1. Introduction

2. Definitions

3. Data Controller

4. Collection Methods

5. Personal Data Collected

6. Purposes of Personal Data Processing

7. Data Sharing

8. International Data Transfer

9. Data Retention and Disposal

10. Personal Data Security

11. Data Subjects' Rights

12. Artificial Intelligence

13. Changes to this Notice

1 Introduction

At CloudWalk, your privacy and the protection of your personal data are priorities. We understand that the recruitment process involves sharing important information, and we want to ensure complete transparency about how we collect, use, store, and protect your data.

This Privacy Notice for Candidates clearly explains how we process your information throughout the recruitment stages, in compliance with the General Data Protection Law (LGPD – Law 13.709/2018) and other applicable regulations. Our commitment is to handle your data securely and responsibly, respecting your rights as a data subject.

2 Definitions

Artificial Intelligence (AI): A field in computing that develops systems and algorithms capable of performing tasks that usually require human intelligence, including learning, reasoning, pattern recognition, decision-making, and natural language processing.

ANPD: The National Data Protection Authority, the public authority responsible for ensuring, implementing, and supervising compliance with the LGPD across the national territory.

Candidate: Any individual who has voluntarily expressed interest in working at CloudWalk or has been selected and/or referred to participate in a recruitment process.

Controller: A natural or legal person, public or private, responsible for decisions regarding the processing of personal data.

Data Protection Officer (DPO): The person designated by the controller and processor to act as the communication channel between the controller, data subjects, and the ANPD.

Data Subject: The natural person to whom the personal data refers—in this case, the candidate.

LGPD: The Brazilian General Data Protection Law No. 13.709/2018, which governs the processing of personal data in physical and digital media by both companies and public bodies. Its main objective is to ensure greater security, transparency, and control for data subjects.

Personal Data: Any information relating to an identified or identifiable natural person. Examples include name, surname, date of birth, address, phone number, email, bank details, employee ID, position, salary information, CPF, and RG.

Processing: Any operation carried out with personal data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation, control, modification, communication, transfer, dissemination, or extraction.

Processor: A natural or legal person who processes personal data on behalf of the controller, following their instructions.

Sensitive Personal Data: Personal data relating to racial or ethnic origin, religious belief, political opinion, union membership, or affiliation to a religious, philosophical, or political organization; data concerning health or sex life; genetic or biometric data when linked to a natural person

3 Data Controller

We act as the controllers of personal data collected in the recruitment and selection context. This means we are responsible for all processing activities involving candidates' personal data, even if carried out by third parties acting as processors.



4 Collection Methods

The personal data necessary for conducting the recruitment process may be collected from the following sources:

- Direct application on our website;
- Internal referral by an employee;
- Active search conducted by internal recruiters or specialized partners;
- Internal application by employees interested in new opportunities.

Regardless of the collection method, all data is securely stored in our Talent Bank. Candidates can request its removal at any time. This data is accessible only to recruiters, managers, and the Attraction and Selection team for future opportunities that match specific job requirements. The retention period is detailed in section 9 of this notice.

5 Personal Data Collected

To ensure a better and more accurate selection process, we may collect the following personal data:

- Registration data such as full name, email address, home address, phone number, date of birth, gender, and national identifiers (CPF, RG, or passport number).
- Sensitive personal data such as disability status for accessibility and inclusion purposes.
- Professional and academic information including details of previous job experiences, academic background, language proficiency, courses, certifications, and other information contained in the resume.
- Information from websites and social media such as LinkedIn, GitHub, and professional portfolios.
- Information collected during interviews such as screen captures, images/videos, and voice recordings.

Any other data or information that the candidate voluntarily provides during the recruitment process.

6 Purposes of Personal Data Processing

Candidates' personal data is processed exclusively for purposes related to the recruitment process, including:

- Analysis and assessment of the professional profile for job compatibility;
- Contacting candidates to schedule interviews and communicate the application status;
- Interviews with the Attraction and Selection team and relevant managers;
- Conducting case studies and technical tests required for the job;
- Performing professional reference checks;
- Conducting background checks to comply with legal and regulatory obligations;
- Ensuring accessibility and inclusion throughout the recruitment process;
- Improving our internal recruitment process based on internal analyses;
- Maintaining our Talent Bank for consideration in future opportunities;
- Sending offer letters, if the candidate is selected;
- Enabling CloudWalk's regular exercise of rights in accordance with legal obligations.

All candidate personal data is processed for specific purposes based on legal grounds such as contract execution or preliminary contract procedures (art. 7, V), legitimate interest (art. 7, IX), and legal obligations (art. 11, II, 'b').

7 Data Sharing

We may share candidates' personal data in a secure and transparent manner, ensuring compliance with applicable data protection laws. Sharing may occur with:

- Government, judicial, legislative, and regulatory authorities for legal and regulatory compliance or the regular exercise of rights in judicial, administrative, or arbitration proceedings;
- Business partners and service providers such as recruitment platforms and specialized agencies, for executing preliminary procedures related to the recruitment process.

All partners are carefully selected and contractually bound to process personal data in strict compliance with applicable data protection regulations.

8 International Data Transfer

Candidates' personal data may be transferred outside the national territory due to the location of cloud servers we use. In such cases, we ensure appropriate measures are taken to protect candidates' personal information. We also contractually require all data processors receiving such data to demonstrate compliance with applicable privacy and data protection laws, especially the LGPD provisions on international data transfers.

9 Data Retention and Disposal

We understand that candidates who submit their resumes and/or participate in our recruitment processes show interest in future opportunities aligned with their profiles. Therefore, personal data will be stored in our Talent Bank for a defined period of 3 years from the date of the last interaction in the recruitment process, enabling future communication regarding new openings and referencing participation history in past selections.

If a candidate no longer wishes to remain in our Talent Bank, they can request the deletion of their personal data at any time by emailing lgpd@cloudwalk.io.



10 Personal Data Security

We adopt appropriate technical and administrative measures to protect personal data against unauthorized access and accidental or unlawful situations of destruction, loss, alteration, disclosure, or dissemination.

Key security measures include access control and management (ensuring only authorized personnel can access candidates' data), encryption of information in transit (to guarantee data confidentiality during transmission), and anonymization techniques applied after the retention period to permanently disassociate the information from the candidate's identity.

11 Data Subjects' Rights

Under the LGPD, candidates, as data subjects, may exercise the following rights:

Rights	Detailing
Confirmation of data processing	Allows candidates to confirm that their personal data is being processed.
Access to data	Permits candidates to request and receive access to their personal data, subject to trade secrets.
Correction of incomplete, inaccurate, or outdated data	Allows candidates to request correction if their personal data is incorrect, incomplete, or outdated.
Anonymization, blocking, or deletion	Permits candidates to request anonymization, blocking, or deletion of personal data when it is unnecessary, excessive, or processed in violation of the LGPD.
Data portability	Grants candidates the right to data portability to another service provider when regulated by the ANPD.
Deletion of data processed with consent	Permits candidates to request deletion of personal data processed based on consent, except where legal or regulatory obligations require retention or where necessary to protect CloudWalk's rights.
Information about data sharing	Allows candidates to request information regarding the entities with whom their data is shared.
Information on the possibility of withholding consent	Allows candidates to request information about the possibility of withholding consent and the potential consequences.
Withdrawal of consent	Permits candidates to withdraw consent previously given during any stage of the recruitment process.
Review of automated decisions	Allows candidates to request a review of automated decisions affecting their interests.

To exercise any of these rights, contact us at lgpd@cloudwalk.io. We may request identity verification to protect against fraud. Note that these rights are not absolute and may not be fully granted in situations involving trade secrets, legal, or regulatory obligations.

12 Artificial Intelligence

We use technology in our daily operations to optimize various tasks, including recruitment. AI tools may be used to enhance the experience for both candidates and the Attraction and Selection team, for example, through automatic speech-to-text transcription during interviews and verbal analysis to assist interviewers in assessing candidate seniority.

However, AI tools do not replace human judgment. Hiring or candidate continuation decisions are made by recruiters and managers, ensuring a transparent and fair process.

13 Changes to this Notice

We reserve the right to modify this Privacy Notice for Candidates whenever necessary to accurately reflect our data processing practices and comply with applicable laws.

For questions or to exercise your data rights, contact our Data Protection Officer (DPO), Aline Aparecida Fonseca de Lima, at lgpd@cloudwalk.io.

This Privacy Notice was last updated in 2025 April.