Privacy Policy

DOCUMENT REVIEW HISTORY		
Version	***Change***	***Issue Date***
1	Initial Version	06/FEB/2025

1. PRIVACY POLICY – SCOPE

Welcome to FIVE Validation.

This Privacy Policy explains how we collect, use, disclose, and protect the data of users who access the company's website. This document covers potential clients, current clients, and applicants for job opportunities advertised by FIVE.

Additionally, this policy applies to the contact database maintained by the company, including people who have not registered to receive our newsletter or other communications. Please note that your first name, last name, and corporate email address may be included in our database due to interactions conducted prior to the issuance of this policy and/or the implementation of the registration functionality for receiving our content on our website https://fivevalidation.com/.

The FIVE Validation team is committed to adhering to the basic security and privacy requirements defined by the General Data Protection Regulation (GDPR).

The privacy and security of the personal data we collect are priorities. Therefore, this document was prepared to demonstrate our commitment to protecting information, addressing topics such as the rights of data subjects, methods of use, types of data processed, legal bases that legitimize processing, and the contact channels available for exercising rights and clarifications.

2. DEFINITIONS

- **Data Subject**: person whose personal information is being collected, stored, or used. For example, if a company has your name, email, or phone number, you are the Data Subject for that data.
- **Controller**: the natural or legal person, public or private, responsible for decisions regarding the processing of personal data. In other words, you are responsible for making decisions regarding the activity to be carried out with personal data.

- **Processor**: the natural or legal person, public or private, that processes personal data on behalf of the controller and in accordance with the purpose determined by them.
- **Personal Data**: all information or combination of information that can identify a data subject unequivocally, that is, without any doubt.
- **Special Category of Personal Data:** personal data related to racial or ethnic origin, religious belief, political opinion, union membership, or membership in a religious, philosophical, or political organization, data concerning health or sexual life, genetic or biometric data.
- **Data Protection Officer (DPO)**: the individual responsible for acting as a communication channel between the controller, data subjects, and data protection agencies when matters involve personal data.
- **Processing**: any activity involving personal data, including but not limited to collection, production, reception, classification, utilization, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, and evaluation.

3. ABOUT THIS POLICY

This Policy aims to:

(A) Ensure that individuals whose information is collected understand what personal data is processed, the reasons for its use, and whether such information is shared.

(B) Explain how the mentioned personal data is used.

(C) Present the rights and options available to data subjects regarding the collected information and detail the measures taken to protect this data.

4. INDIVIDUAL RIGHTS AND PREFERENCES: FIVE VALIDATION PROVIDES USERS WITH CHOICE AND CONTROL

In accordance with current legislation and respecting potential restrictions, the rights guaranteed to individuals include:

(A) Confirmation and Access: The data subject has the right to verify whether their personal data is being processed by an organization and access this information.

(B) Data Correction: It is possible to request adjustments or updates to incomplete, incorrect, or outdated information.

(C) Data Deletion: The data subject may request the deletion of personal information, if there is no legal basis for its retention.

(D) Objection: It is permissible to contest the processing of personal data, including its use for direct marketing.

(E) Portability: The data subject may obtain a copy of the data in electronic format and transfer it to another organization or service.

(F) Consent Revocation: When the legal basis is consent, its withdrawal can be requested at any time.

(G) Information on Consent and Consequences: The data subject has the right to clear guidance on the option not to provide consent and the potential effects of this decision.

Data subjects can exercise these rights through written communication to the email **contact@fivevalidation.com**. FIVE Validation will respond within 15 days, which may be extended with justification.

5. HOW FIVE VALIDATION COLLECTS PERSONAL DATA

The collection of personal data by FIVE Validation may occur in several ways:

(A) Forms: filling out forms on the company's website.

(B) Partners: obtaining information from third parties such as partners with whom it collaborates.

(C) Services: obtaining data from client employees related to ongoing or completed projects.

(D) Contracts: information about contract signatories, such as legal representatives and witnesses.

(E) Cookies: using cookies to enhance users' browsing experience on its website.

(F) Events: collecting data during events it participates in or organizes, with the aim of maintaining contact with interested participants.

(G) Recruitment: using third-party software during the recruitment process to select candidates, conduct interviews, and make hires.

Whenever possible, FIVE Validation uses anonymized and aggregated information for purposes such as testing IT systems, investigation, data analysis, creating marketing and promotional models, improving its software and services, and developing new features and functionalities.

6. PERSONAL DATA PROCESSED BY FIVE

FIVE Validation, in the exercise of its commercial activities, may handle personal data of individuals who have or have had some relationship with the organization, such as clients, business partners, service providers, employees, and associates.

The data processed includes contact information, identification, professional data, and cookies used to enhance the website's user experience.

When acting as a processor, the company limits itself to processing only the data necessary to perform the service, with the controller being responsible for the legal basis and appropriate consent.

In all cases, the company restricts itself to processing the minimum amount of personal data necessary for each process.

7. HOW WE USE YOUR DATA

We use the personal data collected to ensure that you have a safe, efficient, and personalized experience in our interactions. Below are the main ways we use your data:

• To Provide Our Services

We process your data to create and manage your account, respond to requests, or provide support related to our services.

• To Improve User Experience

We use information about how you interact with our services to enhance features, personalize content, and develop new functionalities.

• For Communication

We send important updates, such as notifications about changes to our services, transaction confirmations, or responses to your requests.

We also use your data to send promotional materials or newsletters, but only with your consent, which can be revoked at any time.

• To Comply with Legal Obligations

We use data to comply with applicable regulations, prevent fraud, protect our rights, or respond to requests from competent authorities.

• For Analysis and Statistics

We anonymize and aggregate data to analyze usage patterns and gain insights into how our services are used, without identifying individuals.

• To Ensure Security

We monitor the use of our services to identify suspicious or unauthorized activities and protect your data and our platform from security breaches.

8. HOW WE PROTECT YOUR DATA

• Technological Security Measures

We use advanced encryption protocols to protect your data during transmission and storage, ensuring that sensitive information, such as personal and financial data, remains secure.

• Restricted Access Controls

Only authorized employees who need the data to perform their duties have access to the information, and all undergo regular security and privacy training.

• Continuous Monitoring

We conduct ongoing monitoring and implement threat detection systems to identify and mitigate potential security risks.

• Secure Environments

We host our platforms and data on servers located in data centers that comply with international security standards, such as ISO 27001.

• Regular Testing and Updates

We conduct periodic audits and security tests (including penetration testing) to ensure that our systems are up to date against the latest threats.

• Backup and Recovery

We maintain robust backup systems to protect your data from loss or corruption, ensuring it can be restored in case of incidents.

Although we adopt the best security practices, it is important to note that no system is 100% immune to attacks. Therefore, we continuously monitor our systems and update our practices to minimize any risk as much as possible.

9. FIVE VALIDATION'S ROLE AS CONTROLLER AND/OR PROCESSOR OF PERSONAL DATA

Depending on the established legal relationship, the organization may act as a Controller or Processor of data, as defined in this document and in compliance with the GDPR.

When the company is responsible for determining the purposes, means, and decisions related to data processing, FIVE Validation will be considered the controller. An example is the processing of personal information of its employees.

On the other hand, in cases where data processing is carried out on behalf of a Controller, the organization will assume the role of Processor, such as when processing client employee data during service delivery. Additionally, providers, consultants, and partners may act as Processors when performing processing operations on behalf of the company for its clients.

Regardless of the role performed in its activities, the organization reaffirms, through this document, its commitment to good data governance practices, considering the nature, scope, objectives, risks, and benefits involved in processing data subjects' information.

10. LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

The organization is authorized to process personal data in various situations, such as consent from the data subject; compliance with legal or regulatory obligations; execution of contracts or related activities; protection of life or physical integrity of individuals; defense of legitimate interests, either its own or third parties', provided fundamental rights of data subjects are preserved; and credit protection, as provided by applicable legislation. Additionally, the company implements technical and organizational measures to ensure the security of personal data against unauthorized access. In cases of international transfers, it complies with local laws and takes measures to protect data subjects' rights.

Information sharing may occur in collaboration with fraud investigations, as requested by competent authorities and in compliance with current legislation.

Data is retained for the period necessary for service delivery, compliance with legal requirements, and legitimate business objectives. After these purposes are concluded, information is discarded if there is no legal basis for its retention.

The security of information is a priority, with policies and technical solutions implemented to protect it. Contract templates have been reviewed, incorporating specific confidentiality and data protection clauses, and suppliers are evaluated for the security they offer in handling personal information.

11. HOW LONG WE WILL RETAIN YOUR DATA

We retain your corporate email address for communication and marketing purposes as long as you maintain your authorization. Your data will be deleted as soon as you revoke your authorization or when the provided email becomes invalid, whichever comes first.

You can revoke your authorization at any time by clicking the unsubscribe link available in the footer of our marketing messages or by accessing the Newsletter page on our website. After revocation, your data will be securely deleted from our systems unless there is a legal obligation to retain it.

For legal or regulatory purposes, your data may be stored for additional periods as required by applicable law.

12. CHANGES TO THE PRIVACY POLICY

FIVE Validation reserves the right to amend this document at any time, at its sole discretion or due to regulatory updates.

The provisions of this document will take effect immediately upon publication on the company's website.

13. DATA PROTECTION OFFICER (DPO)

The role of the Data Protection Officer (DPO) is designated by the Controller to serve as a communication channel between the Controller, data subjects, and data protection agencies.

You can contact our Data Protection Officer at **dpo@fivevalidation.com** for matters related to the processing of personal data.

14. REMOVAL OF PERSONAL DATA OF JOB APPLICANTS

If a candidate applying for a job opportunity at FIVE Validation is not hired and wishes to have their personal data removed from our records, they may request deletion by sending an email to **recrutamento@fivevalidation.com**. Upon request, the data will be securely deleted, in compliance with applicable legal deadlines.

15. HOW TO CONTACT US

Thank you for reading FIVE Validation's Privacy Policy.

For any questions about this document or how personal data is processed by the organization, you can contact us at **contact@fivevalidation.com**.