



GO!FIVE® Data Privacy Policy

www.fivevalidation.com

FIVE Validation

This document is CONFIDENTIAL and must not be reproduced, copied, totally or partially changed, published to organizations other than the recipient's company without the express and formal permission of FIVE.

Summary

1	DOCUMENTATION REGISTRY.....	3
2	GENERAL CONSIDERATIONS	5
2.1	OUR SERVICES INCLUDE:	5
3	DATA SEGREGATION	6
3.1	DATA THAT MAY BE COLLECTED.....	6
3.2	REGISTRATION DATA	6
3.3	DATA COLLECTED DURING USE OF GO!FIVE®	6
3.4	WHY GO!FIVE® COLLECTS DATA	7
3.5	AUDIT AND TRACEABILITY DATA (AUDIT TRAIL).....	7
3.6	TECHNICAL AND SYSTEM USAGE DATA	7
3.7	LOCATION DATA.....	8
3.8	POTENTIALLY SENSITIVE OR REGULATED DATA.....	8
3.9	PROVIDING OUR SERVICES.....	8
3.10	CONTACTING USER	9
4	DATA EXPORT	9
5	DATA DELETION	9
6	DATA TRANSFER	10
7	DATA STORAGE AND RETENTION	10
8	DATA SHARING BY THE USER.....	11
9	DATA SECURITY.....	11
10	REQUEST FOR ASSISTANCE FROM THE GO!FIVE® SUPPORT TEAM.....	12
11	INFRASTRUCTURE PROVIDER	12
12	DATA SHARING FOR LEGAL REASONS	13
13	IN THE EVENT OF A MERGER, ACQUISITION, OR SALE	13
14	DATA SUBJECTS' RIGHTS AND DATA PROTECTION OFFICER (DPO).....	13
15	SECURITY INCIDENT MANAGEMENT AND NOTIFICATION.....	14
16	ABOUT THIS POLICY	15
17	TERMS AND DEFINITIONS.....	15

1 Documentation Registry

DOCUMENT REVIEW HISTORY		
Version	Details	Issue Date
1	Document issued for FIVE approval.	17/MAY/2019
2	e-mail update on topic 2, from helpdesk.go5@fiveconsultoria.com to helpdesk.go5@fivevalidation.com ; Addition of registered trademark of GO!FIVE™.	29/SEP/2021
3	Changes made according to occurrence 23-00056: • Change from GO!FIVE™ to GO!FIVE® throughout the document. • Formatting adjustments in the document. • Changed item A of topic 10. Data Security.	01/SEP/2023
4	Change Control 26-00040 - Complete revision of the document. Restructuring and expansion of Section 4—Data That May Be Collected, with the creation of subsections 4.1 through 4.7 for greater detail and clarity. Update to topic 4.8, with the description of data use adapted to system functionalities. Incorporation of the Data Governance Section, with a description of information classification practices, the data lifecycle, and responsibilities. Separation of data sharing into two distinct sections: by the User and by FIVE (Controller and Processor). Revision of Section 2 – General Considerations to reflect FIVE's role as a Data Processor under the LGPD and other applicable privacy regulations. Update to the Security Section with details on cryptographic mechanisms (TLS 1.3) Inclusion of an explanatory note on Tenants in Section 3. Inclusion of DOCX and CSV in Section 5. Update to Topic 7 regarding international data transfers, compliance with the LGPD and international regulations, and removal of outdated references. Revision of Section 9, refining guidance related to data sharing by users and reinforcing the responsibilities of the contracting organization. Inclusion of a new Topic 12, "Security Incident Management and Notification", with renumbering of subsequent sections accordingly.	06/Aug/2026

	Revision and expansion of the Terms and Definitions section, including an updated glossary with privacy, regulatory, and technical terminology. General renumbering of sections to accommodate the new content. General organizational adjustments to the document to improve readability. Updated the table of contents to reflect the new structure. Changes implemented according to Change Request 26-00045: Deployment of a dedicated instance in the AWS eu-west-1 (Ireland) region, 100% independent from the U.S. instance (with its own VPC, database, storage, and authentication), without data migration or cross-region replication. Updated the Data Transfers section to reflect the multi-regional model (US and EU) and GDPR-equivalent treatment for European customers. Included a list of subprocessors by region (AWS; Balsoft/ConvertAPI for document conversion, with a dedicated endpoint in the EU). Revision of the Data Storage and Retention section to clarify that retention periods, deletion requirements, and related conditions are contractually defined and that customers may choose whether their data is stored in the US or the EU environment. Addition of a comprehensive Data Subjects' Rights section covering rights established under the GDPR (Articles 15–22) and LGPD (Article 18). Revision of the Data Protection Officer (DPO) and Security Incident Management and Notification sections to address GDPR requirements applicable to European customers, including 72-hour incident notification obligations and evaluation of EU representative requirements. Expansion of the Terms and Definitions section to include terminology associated with the multi-regional architecture and international data protection frameworks.	
5	General review and update of the document's sections as already described in Revision 4. Change of 'working days' to simple days' in section 14: Rights of Data Subjects and the Data Protection Officer (DPO).	03/SET/2026

2 General considerations

This Privacy Policy aims to clearly and transparently describe how GO!FIVE® collects, uses, stores, protects, and shares data.

GO!FIVE® is software used for validation lifecycle management, assisting users in meeting regulatory requirements and successfully conducting audits.

The software is designed to support data related to validation processes and is not intended for the storage of sensitive personal data or high-risk confidential information (such as patient data or confidential company information, including production orders, product data, formulations, etc.).

However, due to the nature of validation processes, customers may insert actual data as evidence, particularly during phases in which systems are already operating in production environments. In such cases, the customer is responsible for ensuring the suitability, necessity, and legality of the inserted data.

Validation data is stored in a segregated environment within the customer's tenant. Access is restricted to authorized users, and data is not disclosed to third parties unless required by contract or legal obligation. **Note:** A tenant refers to a logically segregated section of a database, exclusively accessible by the contracting customer, including its own dedicated URL.

FIVE Validation acts as a Data Processor, storing, organizing, and making information available according to customer instructions. The customer acts as the Data Controller and is responsible for determining purposes and ensuring the legitimacy of the data entered.

Data processed within GO!FIVE® is used exclusively for:

- Execution of contracted services
- Compliance with regulatory requirements and audits
- Proper operation of the system
- Information security and incident prevention

FIVE does not:

- Sell data.
- Share data without authorization.
- Use data for purposes other than those described in this Policy.

FIVE may use anonymized data, without the possibility of identifying data subjects, exclusively for continuous improvement of the platform and development of new features.

For questions or concerns, users may contact the official support channel: helpdesk.go5@fivevalidation.com.

2.1 Our services include:

- GO!FIVE® Platform - Validation Lifecycle Management System.
- GO!FIVE® WIKI - Online support platform.

- Specialized support services.

3 Data segregation

Data is segregated through a dedicated tenant architecture, ensuring:

- Logical isolation between customers
- Role-based access control
- Restriction of data access to authorized users only

FIVE does not access customer data without:

- Formal authorization.
- Justified operational necessity.

All access is logged and auditable.

Personal data processed within GO!FIVE® is limited to system-user information, namely customer employees whose data is required for authentication, traceability, and auditing activities to meet contractual and regulatory obligations. FIVE does not access, process, or assume responsibility for business data entered on the platform by customers. Ownership, adequacy, and compliance with such data remain solely the responsibility of the Data Controller.

3.1 Data that may be collected

Data processed by GO!FIVE® falls into two distinct categories: (i) Operational system-user data collected by FIVE in its role as Data Processor, necessary for platform operation, security, and traceability. (ii) Business data entered by customers in their role as Data Controllers as part of validation processes, for which the customer bears exclusive responsibility regarding legitimacy, adequacy, and compliance.

The specific data processed may vary depending on user access profile, contracted services, and system usage context.

Data processed by GO!FIVE® is classified into the categories described below.

3.2 Registration Data

When creating a GO!FIVE® account, users provide information required for identification and system access, including:

- Full name
- Corporate email address
- Access credentials

This information is used exclusively for access control, authentication and, traceability of system activities.

3.3 Data collected during use of GO!FIVE®

During system use, data entered by customers as part of validation processes may be collected and stored, including:

- Documents and protocols
- Test evidence
- Execution records
- Attachments and validation-related files

This information reflects the validated environment of operations and is entered under the customer's responsibility. Customers must ensure data accuracy, appropriateness, legality, and regulatory compliance.

Within the customer's tenant, such information is accessible exclusively to authorized users.

FIVE may access this information only when formally authorized or when operationally necessary, as provided in this Policy.

3.4 Why GO!FIVE® Collects Data

Collected data is used exclusively to:

- Deliver contracted services.
- Enable validation process management and execution.
- Ensure platform functionality.
- Meet regulatory and audit requirements.
- Support technical support activities and incident investigations.
- Improve system performance and usability.

Where applicable, FIVE may use data in anonymized form to continuously improve the platform without identifying data subjects.

3.5 Audit and Traceability Data (Audit Trail)

The system automatically records activity logs, including:

- System access events
- Data and document modifications
- Record additions and deletions.
- Audit-relevant actions.

These records are used to ensure traceability, data integrity (ALCOA++) and, compliance with regulatory requirements (GxP).

3.6 Technical and System Usage Data

Data may be automatically collected to ensure the proper operation of the platform, including:

- System logs
- Session information
- Performance and operational data

This information is used exclusively for:

- System monitoring
- Information security
- Incident diagnosis and troubleshooting

3.7 Location data

FIVE does not collect user location data.

IP addresses may be automatically recorded by logging and monitoring systems exclusively for information security purposes, such as detecting suspicious or unauthorized access attempts. IP addresses are not used for user tracking, profiling, or geolocation identification.

IP addresses are treated as operational technical data and are subject to the same security measures and access controls described in this Policy.

3.8 Potentially Sensitive or Regulated Data

GO!FIVE® was not designed for storing sensitive personal data or critical business information. However, such data may be entered into by customers as part of validation evidence when technically necessary.

In such cases, the contracting customer acts as the Data Controller and is solely responsible for:

- Ensuring an appropriate legal basis for processing
- Assessing the necessity, adequacy, and proportionality of the data entered
- Complying with applicable legal, regulatory, and data protection requirements

FIVE acts as a Data Processor, processing data exclusively according to the Controller's instructions and assuming no responsibility for the content entered or for determining the purposes or legal basis of processing.

For operational data collected directly by FIVE in its role as Processor (including: Registration data, Authentication information, System logs, Audit trail records) processing is based on:

- Performance of the contract with the customer
- Compliance with applicable legal and regulatory obligations pursuant to Article 7 of Brazil's LGPD and, where applicable to data subjects within the EU instance, Article 6 of the GDPR.

Whenever possible, data anonymization measures are recommended, particularly within regulated environments.

Customers should recognize that functionalities such as data exports and external data sharing may increase risks associated with processing this information and are responsible for applying appropriate security controls outside the platform environment.

FIVE stores information exactly as entered by customers while maintaining the security, segregation, and traceability controls defined in this Policy.

3.9 Providing our services

We may use data to provide GO!FIVE® functionalities that assist users in creating validation documentation through suggestions and supporting content.

Where applicable, such data is used in aggregated form or without direct identification, in accordance with the guidelines established in this Policy.

3.10 Contacting user

We may use collected data, such as corporate email addresses, to communicate directly with users. For example, we may send notifications if suspicious activities are detected, such as attempts to log into an account simultaneously with the legitimate account owner.

We may also inform users about future changes, updates, or improvements to our services.

If a user contacts the GO!FIVE® support team, we will retain a record of the request to resolve any reported issues and improve service quality.

3.10.1 Protect GO!FIVE® and our users

We may use data to help improve the security and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that may affect GO!FIVE® or its users.

We use various technologies to process data for these purposes.

We use cookies for cache memory storage related to the user's active session. This storage is necessary for the proper functioning of the system and may include information such as the last project accessed and the last subproject accessed. GO!FIVE® does not analyze or retain this information for analysis.

We will request user authorization before using data for purposes not covered by this Privacy Policy.

4 Data export

Users may export approved records and documents in PDF format. Depending on the subscribed plan, users may also export data in structured formats such as DOCX and CSV. GO!FIVE® does not retain exported files, regardless of their format.

After exporting, the files become the sole responsibility of the user, who must store them within their own environment according to their organization's Information Security and Information Technology policies.

GO!FIVE® retains only the data stored in its database and is not responsible for the custody, storage, backup, or preservation of exported files, including PDF, DOCX, and CSV documents. Management and retention of exported documents are not the responsibility of FIVE.

5 Data deletion

Users with deletion permissions may:

Search for and delete specific items within the system. Delete entire projects and subprojects directly through the system.

Records approved through electronic signatures cannot be deleted by users, in accordance with integrity and record immutability requirements established under FDA 21 CFR Part 11.

Every deletion performed by an authorized user is recorded in the audit trail and includes, at a minimum: Identification of the responsible user, date, time, and deleted item.

We implement technical and organizational measures to protect data against accidental or malicious deletion.

As a result, there may be a delay between a user's deletion request and the effective removal of the corresponding data from GO!FIVE® systems and backups.

Audit trail logs, access history, and other traceability metadata generated by the system cannot be deleted by either users or administrators. These records are retained for periods defined according to: Information security requirements, Audit requirements, Applicable legal obligations, Applicable regulatory obligations.

Users may also be deactivated within GO!FIVE® without removing historical audit records associated with their activities.

6 Data Transfer

GO!FIVE® operates under a multi-regional architecture that includes a United States (US) instance and a dedicated AWS eu-west-1 (Ireland) instance for customers requiring European Union (EU) data residency. Each instance is completely independent, including infrastructure, databases, storage, and authentication services. Customer data remains exclusively within the region defined by contract and is not migrated or replicated across regions.

For data stored within the EU processing is conducted in accordance with the General Data Protection Regulation (GDPR).

Where applicable, appropriate safeguards may be used for international data transfers, including Standard Contractual Clauses (SCCs), particularly when remote support is provided by FIVE personnel located outside the European Union.

For data stored within the US instance, international transfers are performed in accordance with Brazil's General Data Protection Law (LGPD - Law No. 13,709/2018).

Requests from foreign governmental authorities regarding data stored within the EU instance will be assessed according to the data protection laws applicable to the storage region, including GDPR Article 48 and contractual commitments established with infrastructure providers.

We work with infrastructure providers that implement security controls aligned with recognized information security standards.

FIVE utilizes providers that maintain internationally recognized certifications, including ISO/IEC 27001 and SOC reports.

Additional information regarding infrastructure providers is described in Section 12 of this Policy.

7 Data storage and retention

FIVE stores' data in GO!FIVE® for as long as necessary to fulfill the purposes described in this Policy and contractual obligations agreed with the customer acting as Data Controller.

Retention periods, deletion conditions, and other obligations relating to data processing are defined in each customer's contract, subject to applicable legislation. In the event of any conflict, contractual provisions shall prevail.

Contractual arrangements may vary among customers: some contracts require data deletion upon termination or others do not impose such requirements.

In all cases, the governing contract shall determine the applicable retention rules.

Customers may contractually choose their preferred data storage region: United States (US) Or European Union (EU). Each customer environment operates exclusively within the selected region, without replication or transfer of data to the other region.

Upon contract termination or expiration of the applicable retention period, data is securely deleted or anonymized unless legal or regulatory obligations require longer retention.

Specific retention criteria applicable to each contract are documented in the relevant contractual agreements and may be reviewed by customers through audit activities.

8 Data Sharing by the User

When using system functionalities that allow data to leave the platform environment, such as PDF exports, report generation, or record copying, the user assumes full responsibility for the processing of such information outside the controlled environment of the platform.

The user and the contracting organization are responsible for ensuring that data is shared only with authorized recipients and for legitimate purposes. They must apply appropriate security controls to exported files, refrain from disclosing data related to other users, projects, or organizations present in the system, and comply with the contracting organization's internal information security policies and applicable regulatory requirements.

FIVE is not responsible for the use, storage, or sharing of data performed outside the platform environment. Such management remains the sole responsibility of the contracting organization in accordance with its internal policies and legal obligations.

Sharing data originating from the contracted service with third parties or competitors of FIVE is not permitted without the formal consent of FIVE.

9 Data Security

We incorporate security into our services to protect data.

All FIVE products are developed with robust security features that continuously protect data. The insights we receive into the maintenance of our services help us automatically detect and block the security threats that reach the user. And if we detect something dangerous and worthy of notification, we will notify and guide the user about the steps necessary to keep security.

We work hard to protect the user and GO!FIVE® from unauthorized access, alteration, disclosure, or destruction of the data we hold, which includes:

- A) Use of encryption on sensitive static data and use of SSL and TLS 1.3 HTTP in transit encryption.
- B) Use of infrastructure providers that have physical security measures to prevent unauthorized access to our system.
- C) Restriction on data access by employees who need this data to process them, for example, system developers. All employees with this access undergo strict contractual obligations of confidentiality and should be disciplined or dismissed if they fail to comply with these obligations.

10 Request for assistance from the GO!FIVE® Support Team

When necessary to provide support, an authorized employee of FIVE Validation may access data stored within the Customer's tenant exclusively for the purpose of analyzing, diagnosing, and resolving the request submitted by the user.

11 Infrastructure Provider

FIVE uses Amazon Web Services (AWS) as its cloud services provider, which has been duly qualified to host GO!FIVE®.

AWS provides the infrastructure required for data storage, processing, and availability under a shared responsibility model.

FIVE applies technical and security criteria when selecting service providers, prioritizing solutions that comply with internationally recognized information security standards and industry best practices, including recognized certifications.

The US instance is hosted in an AWS region located in the United States. The dedicated instance intended for customers requiring data residency within the European Union is hosted in AWS Region eu-west-1 (Ireland), with Virtual Private Cloud (VPC), database, storage services (S3 buckets), and user authentication services (Amazon Cognito) fully independent from the US instance. No data migration or replication occurs between instances. Backups for each instance remain stored within the same region as the originating data.

For internal administrative purposes, authorized members of the FIVE administrative team (ADM) access the environment through corporate authentication using Azure Active Directory (SSO), which may differ from the authentication mechanisms used by end users of customer organizations: end-user accounts are segregated by region, accounts registered within the EU instance are neither shared nor synchronized with accounts in the US instance, and vice versa.

Subprocessors used by GO!FIVE®:

- Amazon Web Services (AWS): cloud infrastructure services, including computing, storage, and availability, operating in the United States region (US instance) and eu-west-1, Ireland (EU instance); certifications include ISO/IEC 27001.

- Balsoft (ConvertAPI): document conversion service (DOCX to PDF) used by GO!FIVE® functionalities. The provider is ISO 27001 certified and GDPR compliant. The provider does not perform persistent storage of processed documents.

Any changes to the list of subprocessors will be communicated to contracting customers, who may exercise their right to object in accordance with the applicable contractual provisions.

12 Data sharing for legal reasons

We may share a user's personal data outside GO!FIVE® whenever we believe, in good faith, that such access, use, storage, or disclosure is necessary to comply with legal or regulatory obligations or lawful requests from competent authorities.

We may also disclose information when necessary to comply with judicial or administrative proceedings or to protect the rights, security, or integrity of GO!FIVE®, its users, or third parties. Whenever legally permitted and technically feasible, the data subject will be informed about such disclosure, including the purpose of the disclosure and the applicable legal basis.

Notification may be omitted when prohibited by law, regulation, or an order issued by a competent authority.

13 In the event of a merger, acquisition, or sale

If FIVE becomes involved in a merger, acquisition, or asset sale, we will continue to ensure the confidentiality of data and will notify affected users before any data is transferred or becomes subject to a different privacy policy.

14 Data Subjects' Rights and Data Protection Officer (DPO)

FIVE recognizes and respects the rights of personal data subjects established by applicable legislation, including Brazil's General Data Protection Law (LGPD, Article 18) and, for data subjects whose data is processed within the EU instance, the European Union General Data Protection Regulation (GDPR, Articles 15 to 22).

Subject to the allocation of responsibilities described in this Policy, under which FIVE acts as the Data Processor and the contracting customer acts as the Data Controller for business data, data subjects may exercise the following rights regarding their personal data:

- Confirmation of processing activities and access to personal data.
- Correction of incomplete, inaccurate, or outdated personal data.
- Anonymization, blocking, or deletion of unnecessary data or data processed in violation of applicable legislation.
- Data portability to another service or product provider upon express request.
- Objection to processing conducted in violation of applicable law and restriction of processing where applicable.

- Information regarding public and private entities with which FIVE has shared personal data.
- Review of decisions based solely on automated processing that affect the interests of the data subject.

FIVE has appointed a Data Protection Officer (DPO) as required by Article 41 of the LGPD and pursuant to Resolution CD/ANPD No. 18/2024.

The DPO serves as the official communication channel between FIVE, data subjects, and the Brazilian National Data Protection Authority (ANPD).

The DPO's responsibilities include receiving and responding to communications and complaints from data subjects, providing guidance to FIVE employees and contractors regarding personal data protection practices, and acting as the primary point of contact with the ANPD.

To exercise the rights listed above or contact the DPO, data subjects must use the official communication channel at DPO@fivevalidation.com, indicating the applicable jurisdiction and the instance in which their data is stored (US or EU).

The response period is up to fifteen (15) days for requests governed by the LGPD (Article 19) and up to one (1) month for requests governed by the GDPR (Article 12), which may be extended by an additional two months when necessary. Additional information regarding the DPO and data protection procedures is available to contract customers through audits. For data subjects and authorities within the European Union, the channel DPO@fivevalidation.com also manages GDPR-related requests. FIVE periodically evaluates the need to appoint a representative within the European Union pursuant to Article 27 of the GDPR, considering the volume and nature of the processing of personal data belonging to European data subjects.

15 Security incident management and notification

FIVE implements appropriate technical, administrative, and organizational measures to prevent, identify, respond to, and mitigate information security incidents that may result in unauthorized access, destruction, loss, alteration, disclosure, or any form of unlawful or improper processing of personal data.

In the event of a security incident involving personal data, FIVE will act diligently to contain its effects, reduce risks, and restore the security of affected environments by adopting, where applicable:

1. Assessment of the nature, scope, and impact of the incident.
2. Implementation of containment, mitigation, and remediation measures.
3. Recording, investigation, and documentation of the incident for audit, compliance, and continuous improvement purposes.
4. Monitoring of corrective and preventive actions intended to avoid recurrence.

Considering its role as Data Processor, FIVE will notify the Customer, acting as Data Controller, without undue delay of any security incident involving personal data processed on the Controller's

behalf or under its responsibility, providing, whenever possible and based on the information available at the time of the notification:

1. The nature of the incident and the personal data involved.
2. The categories of affected data subjects.
3. The risks and potential impacts arising from the incident.
4. The technical and organizational measures adopted or planned for containment, mitigation, and remediation.
5. Any other information necessary for the Controller to assess the incident and fulfill its legal and regulatory obligations.

The Customer, in his capacity as Data Controller, is responsible for determining whether the incident must be reported to competent authorities or affected data subjects in accordance with applicable legislation.

For incidents subject to the GDPR, the Controller must assess whether notification to the competent supervisory authority of the relevant European Union Member State is required pursuant to Article 33 of the GDPR, as well as whether communication to affected data subjects is mandatory under applicable law.

For incidents subject to the LGPD, the Controller must assess whether notification to the Brazilian National Data Protection Authority (ANPD) and affected data subjects is required, observing the applicable legal and regulatory requirements, criteria, and deadlines.

FIVE will cooperate with the Customer in meeting obligations arising from the incident by providing relevant information, updates regarding incident handling, and support consistent with its role as Data Processor.

16 About this Policy

We periodically update this Privacy Policy and ensure that personal data is processed in a manner consistent with its provisions. We will not reduce rights granted under this Privacy Policy without the explicit consent of the contracting organizations. We always indicate the date on which the most recent changes were published and provide access to archived versions for review and reference.

17 Terms and Definitions

Cache:

Memory area where a temporary copy of the data is stored.

Cookie:

A cookie is a small file that contains a string of characters. It is sent to the computer when the user visits a website. When the user accesses the site again, the cookie allows the site to recognize the browser. Cookies can store user preferences and other data. You can configure

your browser to refuse all cookies or to notify you when a cookie is being sent. However, some features or services may not work properly without cookies.

Device:

A device is a computer that can be used to access GO!FIVE®. For example, desktops, laptops, tablets, and smartphones are considered devices.

Personal data:

It is the provided data that identifies the user in person, such as name, surname, and e-mail address.

Sensitive personal data:

This is a specific category of personal data related to topics such as confidential medical data, racial or ethnic origin, political or religious beliefs, or sexuality.

Tenant:

This is a database section of storage for exclusive use of the contractor, or FIVE, when it is designated FIVE's Tenant.

Regional Instance:

A complete and independent GO!FIVE® environment, including infrastructure, database, storage, and authentication services, provisioned in a specific AWS geographic region and intended to serve customers according to their contractual choice of data storage location (for example, the US Instance or the EU Instance).

AWS Region:

A geographically isolated area of data centers operated by Amazon Web Services (AWS). GO!FIVE® uses a region located in the United States for the US Instance and the eu-west-1 region (Ireland) for the EU Instance.

Data Residency:

A legal, regulatory, or contractual requirement that customer data be stored and processed within a specific jurisdiction or geographic region. Within GO!FIVE®, this requirement is fulfilled through the EU Instance, which is dedicated to customers that must keep their data within the European Union.

Subprocessor:

A third party engaged by FIVE to assist with data processing activities related to GO!FIVE®, such as cloud infrastructure providers or document conversion service providers. The list of subprocessors used by GO!FIVE® is described in Section 12 of this Policy.

ALCOA++:

A data integrity principle used in regulated industries, requiring that data be Attributable, Legible, Contemporaneous, Original and Accurate, as well as Complete, Consistent, Enduring and Available.

Anonymization:

A process through which data loses the possibility of being associated, directly or indirectly, with an individual. Anonymized data is not considered personal data under the LGPD.

Audit Trail:

A chronological, automatic, and tamper-evident record of actions performed within a system, including access, additions, modifications, and deletions. It is an essential component of data integrity in GxP systems and a requirement under FDA 21 CFR Part 11.

Data Controller:

A natural or legal person, whether public or private, responsible for decisions regarding the processing of personal data. Within the context of GO!FIVE®, the contracting customer acts as the Data Controller for data entered the platform.

DPO (Data Protection Officer):

An individual appointed by the Data Controller or Data Processor to serve as a communication channel between the organization, data subjects, and the Brazilian National Data Protection Authority (ANPD), pursuant to Article 41 of the LGPD.

BPx:

A collective term used to describe regulated Good Practices established by agencies such as ANVISA, FDA, and EMA, including Good Manufacturing Practices (GMP) and Good Laboratory Practices (GLP). Systems used in GxP-regulated environments must satisfy specific requirements related to validation, data integrity, and traceability.

LGPD / ANPD:

LGPD refers to Brazil's General Data Protection Law (Lei Geral de Proteção de Dados), and ANPD refers to Brazil's National Data Protection Authority (Autoridade Nacional de Proteção de Dados). These terms are comparable to data protection legislation and supervisory authorities in other authorities, including the GDPR framework within the European Union and the Information Commissioner's Office (ICO) in the United Kingdom. A comprehensive directory of global privacy laws and data protection authorities is available through the [Global Privacy Law and DPA Directory | IAPP](#) - Last visited on 06/AUG/2026.

Data Processor:

A natural or legal person, whether public or private, that processes personal data on behalf of a Data Controller. FIVE acts as the Data Processor for data processed within GO!FIVE®.

Data Subject:

A natural person to whom personal data relates. Within the context of GO!FIVE®, data subjects are primarily the users registered in the platform.

TLS (Transport Layer Security):

A cryptographic protocol that ensures the confidentiality and integrity of communications transmitted over the internet. GO!FIVE® uses TLS 1.3, the current and most secure version of the protocol.

Data Processing:

Any operation performed on personal data, including collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation, control, modification, communication, transfer, dissemination, or extraction.

Validation:

A documented process that demonstrates, with a high degree of assurance, that a system, equipment, or process consistently produces results meeting predetermined specifications and quality attributes. Validation is a core activity supported by GO!FIVE®.