



Personal Data Processing and Protection Policy

Last updated: January 2, 2026

INTRODUCTION

In its business operations and provision of technology infrastructure, URL PRO uses a variety of data about identifiable individuals, including:

- Current, former, and prospective employees
- Corporate customers and users of the CPaaS platform
- Users of its websites and omnichannel communication services
- Other interested parties

When collecting, storing, transmitting, and using this data, URL PRO is subject to Colombian legislation regulating how such activities may be carried out and the safeguards that must be put in place to protect the information. The purpose of this policy is to set out the relevant legal guidelines and describe the technical and organizational steps URL PRO takes to ensure compliance. This control applies to all systems, people, and processes that make up URL PRO's infrastructure, including directors, employees, vendors, and third parties who have access to our platforms.

DEFINITIONS

Personal data: Any information related to a natural person that allows that person to be identified or made identifiable, directly or indirectly. This includes name, identification documents, location, biometric data, email addresses, phone numbers, or financial information. This data belongs to its data subject and is protected by law.

Interested parties: Individuals, groups, or organizations that may affect, be affected by, or perceive themselves as affected by the decisions, activities, or results of a company or project. These include internal actors (employees, partners) and external ones (customers, vendors, government, community) that influence sustainability and reputation.

Legal guidelines: Issued when it is necessary to specify or detail actions derived from a higher-ranking instrument such as a Law, a Code, a Regulation, or a Decree, among others.

LEGAL FRAMEWORK (LAW 1581 OF 2012)

The processing of personal data at URL PRO is governed mainly by Statutory Law 1581 of 2012, Decree 1377 of 2013 (compiled into Decree 1074 of 2015), and the guidelines of Colombia's Superintendence of Industry and Commerce (SIC). In addition, given the global scope of its cloud services, URL PRO adopts good practices inspired by the General Data Protection Regulation (GDPR), ensuring a robust level of protection for individual information. URL PRO's strategy is to ensure that its regulatory consistency is clear and continuously verifiable.

3. FUNDAMENTAL CONCEPTS

To properly understand data processing within our CPaaS platform, the following concepts are defined:

Personal data: Any information linked to, or that can be associated with, one or more identified or identifiable natural persons.

Processing: Any operation or set of operations performed on personal data, such as collection, storage, use, circulation, or deletion.

Data Controller: A natural or legal person who, alone or jointly with others, decides on the database and/or the processing of the data. (URL PRO acts as Data Controller with respect to the data of its own employees and direct customers).

Data Processor: A natural or legal person who processes personal data on behalf of the Data Controller. (URL PRO largely acts as Data Processor when it processes communication flows, messages, and end-user data through its omnichannel infrastructure on behalf of its corporate customers).

4. PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA

Under Colombian legislation, URL PRO governs data processing under the following principles:

Legality and Purpose: Processing must serve a legitimate purpose in accordance with the Constitution and the Law, which must be disclosed to the data subject.

Freedom and Consent: Processing may only be carried out with the data subject's prior, express, and informed consent.

Accuracy or Quality: Information subject to processing must be truthful, complete, accurate, up to date, verifiable, and understandable.

Transparency: The data subject's right to obtain information at any time about the existence of data concerning them must be guaranteed.

Restricted Access and Circulation: Personal data may not be made available on the internet or other mass-disclosure media, unless access is technically controllable to provide restricted knowledge.

Security and Confidentiality: Information will be handled with the technical, human, and administrative measures necessary to provide security for records, preventing their alteration, loss, unauthorized consultation, or access.

5. RESPONSIBILITIES OF OUR STAFF

Any URL PRO staff member who takes part in collecting, configuring infrastructure for, storing, or processing data has legal responsibilities. They must ensure that they:

- Obtain and process personal data lawfully.
- Retain such data only for the explicit purposes related to providing the CPaaS service.
- Disclose information only in a manner compatible with the authorized purposes.
- Keep communications infrastructure secure and protected.
- Do not retain data for longer than necessary or than established in service level agreements (SLAs).

6. INDIVIDUAL RIGHTS (HABEAS DATA)

Pursuant to Law 1581 of 2012, the data subject has the right to:

- Know, update, and rectify their personal data held by URL PRO.

- Request proof of the authorization granted.
- Be informed about the use given to their data.
- File complaints with the Superintendence of Industry and Commerce (SIC) for violations of the law.
- Revoke the authorization and/or request the deletion of data when the legal principles are not respected in its processing.

URL PRO's response times, aligned with Colombian law, are as follows:

Data subject request	Legal deadline (Colombia)
Inquiries (Right to know/access)	Maximum of ten (10) business days. May be extended by five (5) more business days if necessary.
Claims (Right to rectify, update, delete, or revoke)	Maximum of fifteen (15) business days. May be extended by eight (8) more business days if necessary.

7. PRIVACY AND SECURITY BY DESIGN

URL PRO has adopted the principle of privacy by design and will ensure that the architecture and planning of all new channels, communication APIs, omnichannel integrations, and databases are subject to a proper impact assessment. This includes:

- Assessing how data flows through the CPaaS infrastructure.
- Implementing end-to-end encryption and secure protocols in communications.
- Using log-minimization and data-masking (pseudonymization) techniques for message histories.

8. DATA PROTECTION OFFICER / AREA

To comply with regulations, URL PRO designates an internal area or Security Officer who will be responsible for processing data subject requests and ensuring compliance with this policy within the company.

9. SECURITY INCIDENT NOTIFICATION

In the event of breaches of security codes or risks in the management of data subjects' information, URL PRO will promptly notify the Superintendence of Industry and Commerce (SIC) through the National Database Registry (RNBD) within fifteen (15) business days following detection of the incident, as well as the affected parties and our corporate customers, activating our Incident Response Procedure.

10. OUR OBLIGATIONS AS A CPAAS AND CLOUD SERVICES INFRASTRUCTURE PROVIDER

In addition to maintaining its own corporate data, URL PRO temporarily or permanently stores and processes the data and communication flows of our corporate customers in the cloud. In our role as Data Processor:

- We provide our customers with the tools and APIs necessary to comply with their legal obligations regarding access, rectification, and deletion of their end users' information.
- We use information routed through our platform exclusively for the technical purposes contracted by the customer, not for our own commercial purposes.

- We do not disclose traffic data or message content, unless a binding legal mandate from Colombian authorities requires it.
- We transparently inform our customers about the use of subcontractors (third-party telecommunications networks or cloud providers) necessary for the platform's operation.
- We immediately notify our corporate customers if their traffic or information is subject to any type of unauthorized access.