Privacy and Personal Data Protection Policy

Defines the mandatory guidelines for the processing, protection, and governance of personal data at PX.Center, in compliance with the LGPD, ISO/IEC 27701:2019, and ISO/IEC 27001:2022.

Code:	*POL-SIP-029*
Responsible area:	*Privacy*
Issue date:	*24/06/2026*
Approval authority:	*DPO / CSIP*

1. PURPOSE/OBJECTIVE

This policy establishes the mandatory guidelines for the processing of personal data by PX.Center, in compliance with Law 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD), ISO/IEC 27701:2019 (Privacy Information Management System, PIMS), and ISO/IEC 27001:2022. PX.Center is responsible for the processing of personal data within the scope of its activities and those of the companies under its management, in the capacity of controller.

This policy defines the permitted legal bases, data subject rights, retention and international transfer rules, security requirements, and the incident notification procedure, ensuring transparency, security, and legal compliance. All employees, service providers, suppliers, and systems that process personal data on behalf of PX.Center are required to operate in compliance with the controls defined herein. This policy derives from the Information Security Policy (POL-SIP-001), to which it is subordinate, and details the processing of personal data within the scope of the SGI.

2. SCOPE/APPLICABILITY

This policy applies to:

a) all employees, interns, and service providers of PX.Center, directly or indirectly;

b) systems, applications, and processes that collect, store, process, transmit, or delete personal data;

c) processing operations carried out on behalf of PX.Center by third parties (processors), under both controller and processor capacities.

This policy covers the entire personal data lifecycle: planning, collection, use, storage, sharing, and deletion, across all business units, technological environments, and third-party relationships. It is subordinate to the Information Security Policy (POL-SIP-001).

3. USERS/TARGET AUDIENCE

All employees, interns, and service providers of PX.Center, area managers responsible for processes involving personal data, the Data Protection Officer (DPO), the Information Security Lead, members of the CSIP (Information Security and Privacy Committee), and third parties who process personal data on behalf of the Organization.

4. REFERENCE DOCUMENTS

- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- ISO/IEC 27701:2019 (Privacy Information Management System)
- ISO/IEC 27001:2022 (Information Security Management System)

- POL-SIP-027: Privacy Governance Policy (PIMS)
- POL-SIP-002: Incident Management Policy
- POL-SIP-012: Personal Device Use Policy (BYOD)
- POL-SIP-017: Training and Awareness Cycle
- POP-SIP-008: Data Subject Request Handling Procedure
- POP-SIP-009: Personal Data Protection Impact Assessment
- INN-RAD-009: Personal Data Protection

5. GUIDELINES / RULES / CONTROLS

5.1 Processing Principles

The processing of personal data at PX.Center observes the principles of Article 6 of the LGPD: purpose, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination, accountability, and answerability. Processing personal data without a defined legal basis and purpose is prohibited. It is mandatory to record the legal basis and purpose of each activity in the Record of Personal Data Processing Operations (ROPA) prior to the start of the operation.

PX.Center periodically evaluates the purposes of its processing operations, considering the context in which they occur, the risks and benefits to the data subject, and the legitimate interest of the Organization.

5.2 Legal Bases

Every personal data processing operation at PX.Center is grounded in one of the legal bases of Article 7 of the LGPD, recorded in the ROPA. The applicable bases for the Organization are:

a) performance of a contract or pre-contractual procedures to which the data subject is a party, including employment relationships;

b) compliance with a legal or regulatory obligation, notably labor, social security, and tax obligations;

c) exercise of rights in judicial, administrative, or arbitration proceedings;

d) pursuit of the legitimate interests of PX.Center or third parties, with due regard for the fundamental rights and freedoms of the data subject, supported by documented assessment;

e) protection of the life or physical safety of the data subject or a third party;

f) protection of health, exclusively in procedures performed by healthcare professionals, health services, or health authorities;

g) credit protection;

h) consent of the data subject — a free, informed, and unambiguous expression of will for a specific purpose — used residually when none of the other bases apply. Consent is recorded

and may be withdrawn at any time by the data subject. The processing of sensitive personal data complies with the specific circumstances set out in Article 11 of the LGPD.

5.3 Collection and Data Minimization

Only data strictly necessary for the declared purpose may be collected. It is the duty of each area manager to periodically review the fields collected and eliminate those that are not necessary. Collection is carried out through the Organization's official channels, always in accordance with the plan recorded in the ROPA.

5.4 Privacy on Social Media and Messaging

When using social media and instant messaging applications, publishing or sharing confidential, restricted, or personal data is prohibited. Employees are not authorized to speak on behalf of PX.Center or about any internal, restricted, or confidential matter on social media or messaging applications, unless expressly authorized by Management.

Internal chat is used exclusively for work-related conversations; sharing personal data beyond the minimum necessary and outside the compatible access level is prohibited. Acceptable use of resources and devices is governed by POL-SIP-013 (Acceptable Use) and POL-SIP-012 (BYOD).

5.5 Data Subject Rights

PX.Center ensures that data subjects may exercise the rights provided under the LGPD and responds to requests within 15 business days through the official channel dpo@px.center, operated by the Data Protection Officer (DPO), in accordance with the procedure detailed in POP-SIP-008. The following rights are guaranteed to data subjects:

a) confirmation of the existence of processing;

b) access to data;

c) correction of incomplete, inaccurate, or outdated data;

d) anonymization, blocking, or deletion of unnecessary, excessive, or non-compliant data processed in violation of the LGPD;

e) portability of data to another service or product provider, upon express request;

f) deletion of data processed on the basis of consent, except where retention is required by law;

g) information about the public and private entities with which PX.Center has shared the data;

h) information about the possibility of withholding consent and the consequences of refusal (Article 18, VII);

i) revocation of consent;

j) objection to processing carried out on a legal basis that does not require consent, in the event of non-compliance with the LGPD (Article 18, IX);

k) review of decisions made solely on the basis of automated personal data processing that affect the data subject's interests, pursuant to Article 20 of the LGPD, with the provision of clear and adequate information about the criteria and procedures used.

Requests involving data whose retention is required by law or by an applicable legal basis are reviewed by the responsible area together with the DPO, who decides on fulfillment in accordance with applicable legislation.

5.6 Retention and Deletion

Personal data is retained only for the period necessary to fulfill the purpose for which it was collected, or for the period required by a legal, regulatory, or contractual obligation, whichever is longer. Once the purpose and applicable legal retention periods have expired, data is securely deleted or anonymized. Retention rules, by data subject category, are as follows:

a) employees and interns: employment-related data is retained for the duration of the employment relationship and for the subsequent statutory limitation and legal periods — in particular, labor, social security, and tax periods — following termination;

b) contracted service providers, suppliers, and processors: data is retained for the duration of the contract and for the limitation periods applicable to the obligations arising therefrom;

c) unsuccessful job applicants: data is retained for the strictly necessary period of the selection process and discarded upon its conclusion, unless specific consent for retention in a talent pool has been obtained.

Detailed retention periods by activity are defined in the ROPA, maintained by the DPO. Retention of personal data beyond the necessary period without a recorded legal basis is prohibited.

5.7 Data Sharing

Sharing of personal data between business units and with third parties is permitted provided that the registered purpose and legal basis are respected, the necessity principle is observed, and sharing is limited to the minimum data strictly required. Sharing with processors occurs under a contract imposing confidentiality and LGPD compliance obligations. All sharing relationships are recorded in the ROPA.

5.8 Information Security

PX.Center employs appropriate technical and organizational measures to protect personal data against unauthorized access, leakage, alteration, loss, and destruction, including:

a) need-to-know access control for personal data, with restrictions on access to systems and files;

b) encryption and pseudonymization applied to personal data, in particular to sensitive data;

c) continuous monitoring of corporate networks and environments;

d) confidentiality agreements signed by employees, service providers, and third parties;

e) storage of data in secure and reliable environments;

f) periodic training and awareness campaigns, integrated into the cycle governed by POL-SIP-017.

Technical privacy controls are implemented by the IT team in alignment with the Information Security Lead and the DPO. Data protection is incorporated from conception and by default (privacy by design and by default), and the performance of controls is subject to post-deployment monitoring as a permanent obligation, in order to verify the effectiveness of measures adopted after each operation goes live.

5.9 International Data Transfer

Transfer of personal data to countries or organizations that do not provide an adequate level of protection recognized by the ANPD is prohibited, except by means of one of the guarantees set out in Article 33 of the LGPD, with formal approval from the DPO and registration in the ROPA.

5.10 Incident Notification

Any security incident involving personal data — leakage, unauthorized access, improper alteration, loss, or destruction — must be reported immediately by the employee to the DPO via dpo@px.center, and handled in accordance with POL-SIP-002 (Incident Management Policy). Information security incidents without a privacy dimension are reported to security@px.center. To open a ticket, the employee registers the incident, indicates the reason "Privacy and Personal Data Protection Violation", completes the applicable Notification Form, and awaits analysis and instructions from the DPO.

The DPO assesses and documents the need to notify the ANPD and the affected data subjects, pursuant to Article 48 of the LGPD, and does so within no more than 72 hours of becoming aware of the incident, in accordance with current ANPD guidance and the provisions of POL-SIP-002. Processing activities with the potential for high risk to data subjects' rights require a Personal Data Protection Impact Assessment (POP-SIP-009) prior to implementation.

6. RESPONSIBILITIES

- Senior Management: assumes the institutional commitment to data protection, formally designates the DPO, provides the necessary resources, and promotes a culture of privacy throughout the Organization.
- Data Protection Officer (DPO): oversees compliance, performs the duties set out in Article 41 of the LGPD, operates the data subject channel dpo@px.center, liaises with the ANPD, keeps the ROPA up to date, and decides on incident notifications. The role is performed under a contract with a specialized Data Protection Officer service (DPO as a service).
- CSIP: deliberates on privacy matters, approves derived policies, and conducts the annual critical review of the PIMS, in accordance with POL-SIP-027.

- Information Security Lead: integrates ISMS controls with personal data protection, operates the security@px.center channel, and supports incident response involving personal data.
- Area Managers: ensure that processes under their responsibility operate with a defined legal basis and purpose, keep ROPA information up to date, request impact assessments where applicable, and ensure their teams' awareness.
- IT: implements technical privacy controls (pseudonymization, encryption, access control, and monitoring) and post-deployment monitoring of processing operations.
- Employees and third parties: processing personal data outside authorized systems and processes is prohibited; each individual has a duty to report any violation or incident to the DPO.

7. RECORDS MANAGEMENT

The ROPA is maintained by the DPO with mandatory semi-annual review; every new operation involving personal data must be registered before going live, with formal approval from the DPO. Data subject requests received via dpo@px.center, impact assessments (POP-SIP-009), and versions of this policy are held in the DPO's custody and in the SGI document repository. Privacy non-conformities are recorded and handled in the corporate non-conformity management tool. Evidence of privacy training follows POL-SIP-017.

Maintaining the integrity of records is mandatory, with access restricted on a need-to-know basis, and records must be available for internal and external SGI audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy takes effect on the date of its publication on the SGI Portal, with indefinite validity, and is reviewed annually or whenever there is a relevant regulatory change to the LGPD, ANPD guidance, applicable ISO standards, the organizational structure, or the scope of the PIMS. Non-compliance with this policy subjects the offender to the disciplinary measures set out in PX.Center's internal regulations.

9. ANNEXES

Annex A — Record of Personal Data Processing Operations (ROPA)

Annex B — Data Subject Rights Request Form

Annex C — PX.Center Personal Data Classification

CHANGE HISTORY

Version	Date	Author	Change Description
00	16/02/2026	SGI	Document creation
01	24/06/2026	SGI	Recoded to acronym-based identifier