Privacy Governance Policy

Privacy governance framework of PX.Center.

Code	POL-SEG-027
Responsible Area	Privacy
Issue Date	June 24, 2026
Approval Authority	DPO / ISPC (Information Security and Privacy Committee)

1. PURPOSE / OBJECTIVE

This policy establishes PX.Center's privacy governance framework, extending the Information Security Management System (ISMS), established by POL-SEG-001 (Information Security Policy) and MAN-SGI-001, into a Privacy Information Management System (PIMS), in compliance with controls 5.2, 5.6, 6.2, and 6.3 of ISO/IEC 27701:2019, with Law 13,709/2018 (Brazilian General Data Protection Law — LGPD), and integrated with ISO/IEC 27001:2022.

This document defines roles, decision-making bodies, and planning and operational control mechanisms that ensure the processing of personal data in accordance with the legal bases and principles of the LGPD. This policy derives from the Information Security Policy (POL-SEG-001), to which it is subordinate.

2. SCOPE / APPLICABILITY

The PIMS covers all PX.Center processes that involve the processing of personal data, in the capacities of both controller and processor, across all organizational units, technology environments, and third-party relationships. PX.Center's designation as the reference entity covers the other CNPJs (Brazilian tax registration numbers) of the group, waiving the need for a separate document per entity. Included are the systems, information assets, and cloud services that support the personal data lifecycle: collection, use, storage, sharing, and disposal.

This policy applies in conjunction with POL-SEG-029 — Privacy and Personal Data Protection Policy, the organization's base standard for personal data processing. It is subordinate to the Information Security Policy (POL-SEG-001) and integrates into the Information Security Management System.

3. TARGET AUDIENCE

Board of Directors; Data Protection Officer (DPO); members of the ISPC (Information Security and Privacy Committee); Information Security Lead; area managers; and all employees and third parties who process personal data on behalf of PX.Center.

4. REFERENCE DOCUMENTS

- Law 13,709/2018 (Brazilian General Data Protection Law — LGPD)
- ISO/IEC 27701:2019 (controls 5.2, 5.6, 6.2, and 6.3)
- ISO/IEC 27001:2022
- POL-SEG-001: Information Security Policy
- MAN-SGI-001: ISMS Manual
- POL-SEG-029: Privacy and Personal Data Protection Policy
- POL-SEG-002: Incident Management Policy
- POL-SEG-017: Training and Awareness Cycle Policy

- POP-SEG-009: Data Protection Impact Assessment (DPIA) Procedure
- POP-SGI-006: Non-Conformity Treatment Procedure
- INN-GRR-009: Personal Data Protection Standard

5. GUIDELINES / RULES / CONTROLS

5.1 PIMS as an Extension of the ISMS

PX.Center extends the ISMS established by POL-SEG-001 and MAN-SGI-001 into a PIMS, in compliance with control 5.2 of ISO/IEC 27701:2019. The PIMS scope covers all processes involving the processing of personal data, both in the capacity of controller and processor. The requirements of ISO/IEC 27001:2022 are interpreted with the privacy extension: wherever the standard refers to information security, it shall be read as information security and privacy. Processing personal data outside the PIMS scope is prohibited.

5.2 Privacy Roles

In compliance with control 6.3 of ISO/IEC 27701:2019, PX.Center maintains formal privacy roles. The Data Protection Officer (DPO) is appointed by the Board through a formal act, with the role fulfilled through a contract with a specialized Data Protection Officer service (DPO-as-a-Service); contact is disclosed via the dpo@px.center channel. The DPO exercises the duties set out in Article 41 of the LGPD:

- Accepts complaints and communications from data subjects, provides clarifications, and takes appropriate action;
- Receives communications from the Brazilian National Data Protection Authority (ANPD);
- Guides employees and contractors on personal data protection practices.

The DPO operates the data subject channel at dpo@px.center, with a response period of 15 business days, and maintains the Record of Personal Data Processing Operations (ROPA). Area managers are responsible for the processing of personal data in the processes under their management, keep the ROPA information for their processes up to date, and notify the DPO of any change in purpose, legal basis, or data sharing.

The ISPC (Information Security and Privacy Committee) is the organization's deliberative body for privacy: it approves standards, arbitrates interpretation conflicts, deliberates on residual risks, and monitors PIMS performance in monthly meetings.

5.3 PIMS Planning and Operational Control

In compliance with control 5.6 of ISO/IEC 27701:2019, the DPO keeps the ROPA up to date; registering every new processing operation before it begins is mandatory. Every new project, product, or service involving the processing of personal data must trigger a Data Protection Impact Assessment (DPIA) before moving to implementation, in accordance with the model defined in POP-SEG-009, under the responsibility of the requesting area manager with support from the DPO.

Processing activities with potential high risk to data subjects' rights require the completion of this assessment prior to implementation. After implementation, assessed processing activities are subject to post-implementation monitoring, with periodic reviews conducted by the DPO together with area

managers, to verify the maintenance of compliance conditions and the effectiveness of controls. Incidents involving personal data follow POL-SEG-002, with a mandatory additional step: the DPO evaluates and documents the need to notify the ANPD and affected data subjects in accordance with Article 48 of the LGPD.

Privacy non-conformities are recorded and handled in the corporate non-conformity management tool, in accordance with POP-SGI-006.

5.4 Privacy Normative Hierarchy

In compliance with control 6.2 of ISO/IEC 27701:2019, the privacy normative framework follows a hierarchy in which:

- This policy governs the governance of the PIMS;
- POL-SEG-029 — Privacy and Personal Data Protection Policy is the base standard for personal data processing, covering data subjects' rights, legal bases, and international data transfers;
- Derived standards such as INN-GRR-009 and POP-SEG-009 specify controls through procedures, instructions, and internal standards.

Conflicts between standards are resolved by the higher-level standard; the ISPC is responsible for deliberating on cases not explicitly addressed.

5.5 Third-Party Processor Due Diligence

PX.Center maintains a formal due diligence process for third-party processors that process personal data on its behalf, applying a privacy compliance questionnaire prior to contracting and throughout the contractual period. The due diligence verifies the processor's adherence to LGPD obligations and applicable information security requirements; its results support contracting decisions and the maintenance of third-party relationships.

5.6 Privacy Awareness

Privacy and personal data protection content is integrated into the training and awareness cycle governed by POL-SEG-017. Participation is mandatory at onboarding and in periodic refresher courses; area managers ensure their teams' participation.

5.7 Social Media Use

The use of social media on behalf of PX.Center is permitted to the Marketing and Commercial business functions, restricted to institutional and commercial purposes, with the disclosure of confidential data or personal data prohibited. For all other employees, personal use of social media on the organization's assets and environments is prohibited. The publication of any content involving personal data must observe the legal bases of the LGPD and the guidelines of this policy and POL-SEG-029.

5.8 PIMS Management Review

The ISPC conducts an annual management review of the PIMS, evaluating the adequacy of the scope, the state of the ROPA, incidents involving personal data, the results of impact assessments, non-conformities recorded in the corporate non-conformity management tool, data subject requests, and

changes in legislation or ANPD guidance. The ISPC records decisions and resulting action plans in meeting minutes.

6. RESPONSIBILITIES

The **Information Technology (IT) department** is the area responsible for ensuring compliance with this policy and is responsible for investigating violations of its provisions; the contact channel for privacy and LGPD matters is dpo@px.center and for information security matters is security@px.center.

The **Board of Directors** approves this policy, formally appoints the DPO, provides the resources necessary for the PIMS, and is responsible for the organization's commitment to the LGPD.

The **Data Protection Officer (DPO)** exercises the duties of Article 41 of the LGPD, maintains the ROPA, operates the data subject channel, conducts liaison with the ANPD, and reports PIMS performance to the ISPC.

The **ISPC (Information Security and Privacy Committee)** deliberates on privacy matters, approves derived standards, conducts the annual PIMS management review, and monitors the execution of action plans.

The **Information Security Lead** integrates ISMS controls with personal data protection, supports the response to incidents involving personal data, and maintains technical alignment with the DPO.

Area managers are responsible for the processing of personal data in their processes, keep ROPA information up to date, trigger the DPIA when applicable, and ensure awareness within their teams.

7. RECORDS MANAGEMENT

PIMS records reside in the following repositories:

- **ROPA:** under the DPO's custody.
- **ISPC meeting minutes, versions of this policy, and impact assessments (POP-SEG-009):** ISMS (SGI) document repository.
- **Privacy non-conformities:** corporate non-conformity management tool.
- **Data subject service records received via dpo@px.center:** under the DPO's custody.
- **Privacy training evidence:** in accordance with POL-SEG-017.

It is mandatory to preserve the integrity of records, with access restricted to those with a need to know, and to keep them available for internal and external ISMS audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on the date of its publication, with indefinite validity. The ISPC reviews the document annually or whenever there is a relevant change in legislation, ANPD guidance, 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 standards.

9. ANNEXES

There are no annexes. Operational PIMS records reside in the systems indicated in the Records Management section (corporate non-conformity management tool and ISMS document repository).

CHANGE HISTORY

Version	Date	Author	Description
00	Feb 16, 2026	ISMS (SGI)	Document creation
01	Jun 24, 2026	ISMS (SGI)	Recodification to acronym-based code