Privacy Governance Policy

Privacy governance framework of PX.Center

Code:	*POL-SIP-027*
Responsible area:	*Privacy*
Issue date:	*24/06/2026*
Approval authority:	*DPO / CSIP*

1. PURPOSE/OBJECTIVE

This policy establishes the privacy governance framework of PX.Center, extending the Information Security Management System (ISMS), instituted by POL-SIP-001 (Information Security Policy) and MAN-SGI-001, into a Privacy Information Management System (PIMS), in conformance with controls 5.2, 5.6, 6.2 and 6.3 of ISO/IEC 27701:2019, with Lei 13.709/2018 (LGPD) and in integration with ISO/IEC 27001:2022.

The 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-SIP-001), to which it is subordinate.

2. SCOPE/APPLICABILITY

The PIMS covers all PX.Center processes that process personal data, in the capacity of both controller and processor, across all units, technological environments and third-party relationships. PX.Center's designation as the reference entity covers the other CNPJs within the group, dispensing with entity-specific documentation. 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-SIP-029 — Privacy and Personal Data Protection Policy, the Organisation's baseline standard for personal data processing. It is subordinate to the Information Security Policy (POL-SIP-001) and is integrated into the Information Security Management System.

3. USERS/TARGET AUDIENCE

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

4. REFERENCE DOCUMENTS

- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- ISO/IEC 27701:2019 (controls 5.2, 5.6, 6.2 and 6.3)
- ISO/IEC 27001:2022
- POL-SIP-001: Information Security Policy
- MAN-SGI-001: SGI Manual
- POL-SIP-029 — Privacy and Personal Data Protection Policy
- POL-SIP-002: Incident Management Policy
- POL-SIP-017: training and awareness cycle

- POP-SIP-009: Personal Data Protection Impact Assessment
- POP-SGI-006: Non-Conformity Treatment
- INN-RAD-009: Personal Data Protection

5. GUIDELINES / RULES / CONTROLS

5.1 PIMS AS AN EXTENSION OF THE ISMS

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

5.2 PRIVACY ROLES

In conformance with control 6.3 of ISO/IEC 27701:2019, PX.Center maintains formal privacy roles. The Data Protection Officer (DPO) is designated by Management through a formal act, with the role fulfilled through a contract with a specialised Data Protection Officer service (DPO-as-a-service), and the contact published at dpo@px.center. The DPO carries out the duties set out in Art. 41 of the LGPD:

accepts complaints and communications from data subjects, provides clarifications and takes the necessary measures; receives communications from the ANPD; guides employees and contractors on personal data protection practices. Operates the data subject channel dpo@px.center, with a response deadline of 15 business days, and maintains the Record of Personal Data Processing Operations (ROPA). Area managers are responsible for the processing of personal data within their processes, keep ROPA information for their processes up to date and notify the DPO of any change in purpose, legal basis or sharing arrangement.

The CSIP is the Organisation's deliberative body for privacy matters: it approves standards, arbitrates interpretation conflicts, deliberates on residual risks and monitors PIMS performance at its monthly meeting.

5.3 PIMS PLANNING AND OPERATIONAL CONTROL

In conformance with control 5.6 of ISO/IEC 27701:2019, the DPO keeps the ROPA up to date; it is mandatory to register every new processing operation before that operation commences. Every new project, product or service involving personal data processing must trigger a personal data protection impact assessment (DPIA) before proceeding to implementation, in accordance with the model defined in POP-SIP-009, under the responsibility of the requesting area manager with support from the DPO.

Processing activities with the potential to pose high risk to data subjects' rights require the completion of this assessment prior to implementation. Following implementation, assessed processing activities are subject to post-implementation monitoring, with periodic review conducted by the DPO in conjunction with area managers, in order to verify that compliance

conditions are maintained and that controls remain effective. Incidents involving personal data follow POL-SIP-002, with an additional mandatory step: the DPO assesses and documents the need to notify the ANPD and the affected data subjects, in accordance with Art. 48 of the LGPD.

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

5.4 PRIVACY NORMATIVE HIERARCHY

In conformance with control 6.2 of ISO/IEC 27701:2019, the privacy normative framework follows a hierarchy in which this policy governs PIMS governance; POL-SIP-029 — Privacy and Personal Data Protection Policy is the baseline standard for personal data processing, covering data subject rights, legal bases and international transfers; and derived standards, such as INN-RAD-009 and POP-SIP-009, detail specific controls through procedures, instructions and internal standards.

Conflicts between standards are resolved by the higher-level standard, with the CSIP responsible for deliberating on cases not addressed by existing rules.

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 duration of the contractual relationship. The due diligence verifies the processor's adherence to LGPD obligations and applicable information security requirements, and its results inform contracting decisions and the continuation 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-SIP-017. Participation is mandatory upon onboarding and at periodic refresher intervals; area managers ensure their teams' participation.

5.7 USE OF SOCIAL MEDIA

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 disclosure of confidential data or personal data prohibited. All other employees are prohibited from personal use of social media on the Organisation's assets and environments. Publication of any content involving personal data must comply with the legal bases of the LGPD and the guidelines of this policy and POL-SIP-029.

5.8 PIMS MANAGEMENT REVIEW

The CSIP conducts an annual management review of the PIMS, evaluating the adequacy of the scope, the state of the ROPA, personal data incidents, 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 CSIP records decisions and resulting action plans in the meeting minutes.

6. RESPONSIBILITIES

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

Management approves this policy, formally designates the DPO, provides the resources necessary for the PIMS and is accountable for the Organisation's commitment to the LGPD.

The Data Protection Officer (DPO) carries out the duties set out in Art. 41 of the LGPD, maintains the ROPA, operates the data subject channel, leads communications with the ANPD and reports PIMS performance to the CSIP.

The CSIP 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 into personal data protection, supports the response to incidents involving personal data and maintains technical alignment with the DPO.

Area managers are responsible for personal data processing within their processes, keep ROPA information up to date, trigger the impact assessment (DPIA) where applicable and ensure their teams' awareness.

7. RECORDS MANAGEMENT

PIMS records reside in the following repositories:

- ROPA: under the DPO's custody.
- CSIP meeting minutes, versions of this policy and impact assessments (POP-SIP-009): 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-SIP-017.

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

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on the date of its publication, with validity for an indefinite period. The CSIP reviews the document annually or in the event of a material change in legislation,

ANPD guidance, organisational structure or the PIMS scope. 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. The PIMS operational records reside in the systems indicated in the Records Management section (corporate non-conformity management tool and SGI document repository).

CHANGE HISTORY

Version	Date	Author	Change Description
00	16/02/2026	SGI	Document creation
01	24/06/2026	SGI	Recoding to abbreviation