Privacy and Personal Data Protection Policy

Establishes the mandatory guidelines for the processing, protection, and governance of personal data at PX.Center, in compliance with the Brazilian General Data Protection Law (LGPD), ISO/IEC 27701:2019, and ISO/IEC 27001:2022.

Code	POL-SEG-029
Responsible Area	Privacy
Issue Date	June 24, 2026
Approval Authority	DPO / ISPC (Information Security and Privacy Committee)

1. PURPOSE / OBJECTIVE

This policy establishes the mandatory guidelines for the processing of personal data by PX.Center, in compliance with Law No. 13,709/2018 (Brazilian General Data Protection Law — 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, acting as data controller.

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

2. SCOPE / APPLICABILITY

This policy applies to:

1. all employees, interns, and service providers of PX.Center, directly or indirectly;
2. systems, applications, and processes that collect, store, process, transmit, or delete personal data;
3. processing operations carried out on behalf of PX.Center by third parties (processors), both in the capacity of controller and of processor.

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

3. TARGET AUDIENCE

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

4. REFERENCE DOCUMENTS

- Law No. 13,709/2018 (Brazilian General Data Protection Law — LGPD)
- ISO/IEC 27701:2019 (Privacy Information Management System)
- ISO/IEC 27001:2022 (Information Security Management System)
- POL-SEG-027: Privacy Governance Policy (PIMS)
- POL-SEG-002: Incident Management Policy

- POL-SEG-012: Personal Device Use Policy (BYOD)
- POL-SEG-017: Training and Awareness Cycle Policy
- POP-SEG-008: Data Subject Request Fulfillment Procedure
- POP-SEG-009: Data Protection Impact Assessment Procedure
- INN-GRR-009: Personal Data Protection

5. GUIDELINES / RULES / CONTROLS

5.1 Processing Principles

The processing of personal data at PX.Center observes the principles of Art. 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. The legal basis and purpose of each activity must be recorded in the Record of Processing Activities (ROPA) before the operation commences.

PX.Center periodically evaluates the purposes of its processing operations, taking into account the context in which they occur, the risks and benefits to the data subject, and the Organization's legitimate interests.

5.2 Legal Bases

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

1. performance of a contract or pre-contractual procedures related to a contract of which the data subject is a party, including the employment relationship;
2. compliance with a legal or regulatory obligation, in particular employment, social security, and tax obligations;
3. the regular exercise of rights in judicial, administrative, or arbitration proceedings;
4. the legitimate interests of PX.Center or third parties, subject to the fundamental rights and freedoms of the data subject, based on a documented assessment;
5. protection of the life or physical safety of the data subject or a third party;
6. protection of health, exclusively in a procedure carried out by health professionals, health services, or a health authority;
7. credit protection;
8. consent of the data subject — a free, informed, and unequivocal expression of will for a specific purpose — used on a residual basis when none of the other bases applies. Consent is recorded and may be withdrawn at any time by the data subject. The processing of sensitive personal data is governed by the specific cases set out in Art. 11 of the LGPD.

5.3 Collection and 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 occurs through the Organization's official channels, always in accordance with the planning recorded in the ROPA.

5.4 Privacy in 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, except when expressly authorized by Management.

The internal chat tool is used exclusively for conversations related to professional activities. Sharing personal data beyond the minimum necessary or outside the compatible access level is prohibited. Acceptable use of resources and devices is governed by POL-SEG-013 (Acceptable Use) and POL-SEG-012 (BYOD).

5.5 Data Subject Rights

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

1. confirmation of the existence of processing;
2. access to the data;
3. correction of incomplete, inaccurate, or outdated data;
4. anonymization, blocking, or deletion of unnecessary, excessive, or data processed in non-compliance with the LGPD;
5. portability of the data to another service or product provider, upon express request;
6. deletion of data processed on the basis of consent, except for the cases of conservation provided for by law;
7. information about the public and private entities with which PX.Center has shared the data;
8. information about the possibility of not providing consent and about the consequences of refusal (Art. 18, VII);
9. withdrawal of consent;
10. objection to processing carried out on the basis of a legal ground that does not require consent, in the event of non-compliance with the LGPD (Art. 18, IX);
11. review of decisions made solely on the basis of automated processing of personal data that affect the data subject's interests, pursuant to Art. 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 an applicable legal basis are analyzed by the responsible area together with the DPO, who decides on fulfillment in accordance with the legislation.

5.6 Retention and Deletion

Personal data is retained only for the period necessary to fulfill the purpose that motivated collection, or for the period required by a legal, regulatory, or contractual obligation — whichever is greater. Once the purpose and applicable legal periods have elapsed, the data is securely deleted or anonymized. Retention rules are as follows, by category of data subject:

1. employees and interns: employment-related data is retained during the employment relationship and for the subsequent limitation and legal periods — in particular employment, social security, and tax periods — following termination;
2. service providers, vendors, and contracted processors: data is retained during the term of the contract and for the limitation periods applicable to the obligations arising from it;
3. candidates in selection processes not hired: data is retained for the period strictly necessary for the process and discarded after its conclusion, unless specific consent is provided for retention in a talent pool.

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

5.7 Sharing

Sharing personal data between business areas and with third parties is permitted provided that the recorded purpose and legal basis are respected, the necessity principle is observed, and sharing is limited to the minimum data that is indispensable. Sharing with processors occurs pursuant to a contract that imposes 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:

1. access control to personal data based on need-to-know, with restricted access to systems and files;
2. encryption and pseudonymization applied to personal data, especially sensitive data;
3. continuous monitoring of corporate networks and environments;
4. confidentiality agreements signed by employees, service providers, and third parties;
5. storage of data in secure and reliable environments;
6. periodic training and awareness campaigns, integrated into the cycle governed by POL-SEG-017.

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

5.9 International Data Transfer

Transfer of personal data to countries or international organizations that do not provide an adequate level of protection recognized by the Brazilian National Data Protection Authority (ANPD) is prohibited, except through one of the safeguards provided for in Art. 33 of the LGPD, with formal approval from the DPO and recording 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 at dpo@px.center and handled in accordance with POL-SEG-002 (Incident Management Policy). Information security incidents not involving privacy are reported to security@px.center. To open a case, the employee registers a ticket, indicates the reason "Privacy and Personal Data Protection Violation," completes the applicable Notification Form, and awaits the DPO's analysis and instructions.

The DPO evaluates and documents the need to notify the ANPD and the affected data subjects, pursuant to Art. 48 of the LGPD, and does so within no more than 72 hours from the moment the incident becomes known, in observance of the ANPD's current guidance and the provisions of POL-SEG-002. Processing operations with potential for high risk to the rights of data subjects require a Data Protection Impact Assessment (POP-SEG-009) prior to deployment.

6. RESPONSIBILITIES

- **Management and Senior Leadership:** Assume the institutional commitment to data protection, formally designate the DPO, provide the necessary resources, and disseminate a culture of privacy across the Organization.
- **Data Protection Officer (DPO):** Supervises compliance, exercises the responsibilities set out in Art. 41 of the LGPD, operates the data subject channel at dpo@px.center, manages communication with the ANPD, maintains the ROPA updated, and decides on incident notification. This function is exercised under a contract with a specialized data protection officer service (DPO-as-a-Service).
- **ISPC:** Deliberates on privacy matters, approves derived policies, and conducts the annual critical review of the PIMS, pursuant to POL-SEG-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 the processes under their responsibility operate with a defined legal basis and purpose, keep the ROPA information updated, request impact assessments when 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; it is each individual's 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 is recorded before entering production, subject to formal approval by the DPO. Data subject requests received at dpo@px.center, impact assessments (POP-SEG-009), and versions of this policy are kept in the custody of the DPO and in the ISMS document repository. Privacy non-conformities are recorded and addressed in the corporate non-conformity management tool. Evidence of privacy training follows POL-SEG-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 ISMS audits.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on the date of its publication in the ISMS Portal, is valid for an indefinite period, and is reviewed annually or whenever there is a relevant regulatory change in 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 Processing Activities (ROPA)
- Annex B — Data Subject Rights Request Form
- Annex C — PX.Center Personal Data Classification

CHANGE HISTORY

Version	Date	Author	Description
00	Feb 16, 2026	ISMS	Document creation
01	Jun 24, 2026	ISMS	Recoding to acronym-based identifier