Privacy by Design and by Default Policy

Mandatory guidelines for incorporating privacy by design and by default into products, systems, and processes at PX.Center that process personal data, covering the seven foundational principles of Privacy by Design, data minimization, de-identification, retention, return, and disposal.

Code	POL-SEG-028
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 incorporating privacy by design and privacy by default into all products, systems, projects, and processes at PX.Center that involve processing personal data.

This document addresses controls 7.4 and 8.4 of ISO/IEC 27701:2019, which require the adoption of privacy by design and by default by the controller and the processor, and Article 46, paragraph 2, of Law No. 13,709/2018 (Brazilian General Data Protection Law — LGPD), which mandates the observance of security and privacy measures from the design phase of a product or service through to its execution. This policy derives from the Information Security Policy (POL-SEG-001), to which it is subordinate.

2. SCOPE / APPLICABILITY

This policy applies to the entire lifecycle of PX.Center's products, systems, applications, integrations, and business processes that process personal data, in situations where the Organization acts as a controller or as a processor.

It covers the phases of conception, development, testing, staging, production, retention, return, and disposal, in on-premises environments and the corporate cloud environments in use. It equally applies to the acquisition of products or services and to the engagement of vendors and service providers involving software programs, new applications, technologies, or services that process personal data. It includes systems and functionalities based on artificial intelligence, to the extent that they process personal data at any stage of their lifecycle.

This policy is subordinate to the Information Security Policy (POL-SEG-001) and is part of the Information Security Management System (ISMS).

3. TARGET AUDIENCE

Technology/Product Lead, development and engineering teams, Information Security Lead, Data Protection Officer (DPO), Information Security and Privacy Committee (ISPC), project managers, and contracted third parties who participate in the development, maintenance, or testing of PX.Center products and systems.

4. REFERENCE DOCUMENTS

- ISO/IEC 27701:2019, controls 7.4 (privacy by design and by default: controller) and 8.4 (privacy by design, retention, return, and disposal: processor)
- ISO/IEC 27001:2022 (Information Security Management System)
- Law No. 13,709/2018 (LGPD), in particular Art. 6 (principles of adequacy and necessity), Art. 38 (Data Protection Impact Assessment) and Art. 46, paragraph 2
- POL-SEG-001: Information Security Policy

- POL-SEG-029: Privacy and Personal Data Protection Policy
- POL-SEG-027: Privacy Governance Policy
- POL-SEG-005: Secure Disposal Policy
- POL-SEG-006: Cryptography Policy
- POL-SEG-007: Secure Development Policy
- POL-SEG-018: Testing and Staging Policy
- POP-SEG-009: Data Protection Impact Assessment (DPIA) Procedure
- POP-SGI-006: Non-Conformity Treatment
- INT-SEG-002: Data Masking in Test Environments
- INN-GRR-009: Personal Data Protection
- MAN-SGI-001: ISMS Manual
- FOR-17-001: Privacy by Design and DPIA Questionnaire

5. GUIDELINES / RULES / CONTROLS

5.1 The Seven Foundational Principles of Privacy by Design

Privacy by Design requires that data protection and privacy be incorporated throughout the entire lifecycle of projects, products, and services — from conception to disposal — with a preventive perspective. Its application observes the following seven foundational principles.

5.1.1 Proactive, Not Reactive; Preventive, Not Remedial

Anticipate and prevent privacy-invasive events before they occur, rather than waiting for the risk to materialize. Applicable technical measures include anonymization or pseudonymization, encryption, assurance of confidentiality, integrity, availability, and resilience of systems, verification and monitoring of the effectiveness of measures, and restricted access to internal and external repositories.

5.1.2 Privacy as the Default Setting

Privacy is integrated into products, systems, and services by default, without requiring any action by the data subject. The data subject receives the product or service with all safeguards activated from the start of development, is informed of what data is collected and for what legitimate purpose, and is not required to take protective action to ensure privacy.

5.1.3 Privacy Embedded into Design

Privacy is an essential component of the core designed functionality, not an add-on after the fact. Any option for sharing data subject information begins restricted, and the options presented must not be biased toward accepting sharing or granting automatic permission.

5.1.4 Full Functionality — Positive-Sum, Not Zero-Sum

Privacy is incorporated into technologies, processes, and systems without impairing their full functionality, accommodating non-privacy-related objectives in a value-adding manner, with documentation of the interests involved and the pursuit of multifunctional solutions that eliminate the need to sacrifice legitimate objectives.

5.1.5 End-to-End Security — Full Lifecycle Protection

Adoption of robust security measures from the start through to the end of processing, ensuring the protection of personal data throughout all phases of its lifecycle.

5.1.6 Visibility and Transparency

Processing practices remain visible and verifiable, supporting accountability and data subject trust, in observance of the LGPD principles of free access, data quality, transparency, non-discrimination, and accountability.

5.1.7 Respect for User Privacy

Primacy of data subject interests through robust privacy defaults, mechanisms for the exercise of their rights, ease of access, and security measures ensuring the confidentiality, integrity, and availability of data throughout its entire lifecycle.

5.2 Privacy by Design

5.2.1 It is mandatory to survey and record privacy requirements at the outset of every project, product, or feature that processes personal data, before any architecture or development decision is made.

5.2.2 Privacy requirements are integrated into project artifacts and follow the secure development lifecycle defined in POL-SEG-007. Cryptographic controls apply in accordance with POL-SEG-006.

5.2.3 The business unit requesting a new project, process, or service that processes personal data must complete the Privacy by Design Questionnaire (FOR-17-001) and submit it to the DPO and the ISPC for evaluation of prerequisites before the activity begins. The evaluation considers the scope, objective, and purpose of the processing; the nature of the data collected; the legal basis adopted; the forms of storage, use, and transfer; the retention period; the form of disposal; and the physical and logical security measures applied.

5.2.4 A Data Protection Impact Assessment (DPIA) is mandatory, pursuant to POP-SEG-009 and Art. 38 of the LGPD, when the processing is likely to generate high risk to data subjects, including large-scale processing of sensitive data, use of new technologies, or systematic monitoring of data subjects. In other cases, the DPO evaluates and records the decision on the necessity of a DPIA.

5.2.5 The DPO and the ISPC may recommend adjustments, approve, or veto a project — even temporarily — following the analysis of risks and applicable mitigation mechanisms.

5.2.6 It is prohibited to place into production any product or feature that processes personal data without the privacy requirements having been implemented and verified.

5.2.7 After deployment, the project, process, or service that processes personal data is monitored for its development and performance. Post-deployment monitoring is conducted at a minimum once a year and, whenever necessary, more frequently, under the coordination of the DPO and the ISPC, with a view to continuous improvement in accordance with the PDCA cycle.

5.3 Privacy by Default

5.3.1 Every default configuration of a product, system, or feature must be the most restrictive in terms of privacy. Data sharing, profile visibility, and additional collection remain disabled by default and require an affirmative action by the data subject.

5.3.2 The collection of personal data is limited to the minimum necessary to fulfill the declared purpose. It is prohibited to collect personal data without a declared, recorded, and legitimate purpose, in observance of the principles of adequacy and necessity (Art. 6, items II and III, of the LGPD).

5.3.3 Optional data collection fields must be identified as such and must not condition the use of the product when they are not essential to the purpose of the processing.

5.4 Minimization and De-identification

5.4.1 Development teams must anonymize or pseudonymize personal data when the purpose of the processing allows, with priority given to anonymization.

5.4.2 Pseudonymization requires the segregated storage of additional information that would enable re-identification, with restricted access control and usage logging.

5.4.3 It is prohibited to retain identifying attributes in analytical or statistical databases when the purpose can be fulfilled with de-identified data.

5.5 Retention and Disposal

5.5.1 Personal data is retained only for the period necessary to fulfill the purpose of the processing or to comply with a legal or regulatory obligation. Once the purpose has been fulfilled, it is mandatory to delete or anonymize the data, in conformity with control 7.4 of ISO/IEC 27701:2019.

5.5.2 Retention periods by category of personal data are set out in a specific retention schedule. The retention schedule is maintained and published by the Data Protection Officer (DPO) and reviewed every twelve months.

5.5.3 The disposal of personal data and of the media containing it follows the secure disposal procedures defined in POL-SEG-005, with a formal record of the deletion.

5.6 Return and Deletion at End of Contract

5.6.1 In contracts where PX.Center acts as a processor, upon termination of the services, it is mandatory to return to the controller or delete the personal data processed, as per the controller's documented instruction, in conformity with control 8.4 of ISO/IEC 27701:2019.

5.6.2 Deletion must be formally evidenced to the controller. Backup copies containing the data follow the same deletion regime at the end of their retention cycle.

5.6.3 Retention of data after contractual termination is only permitted under a legal or regulatory obligation, which must be formally communicated to the controller.

5.7 Personal Data in Development and Testing

5.7.1 It is prohibited to use real personal data in development, testing, or staging environments without masking, applied in accordance with INT-SEG-002.

5.7.2 Testing and staging environments observe the segregation and access controls defined in POL-SEG-018.

5.8 Artificial Intelligence and Privacy by Design

5.8.1 Systems, features, and agents based on artificial intelligence that process personal data must fully comply with the seven principles in section 5.1 and the controls in this policy, from the conception of the use case.

5.8.2 Completion of the Privacy by Design Questionnaire (FOR-17-001) is mandatory for every artificial intelligence use case that processes personal data. The evaluation must consider the legal basis, minimization of training and inference data, the possibility of de-identification, and the risks of discrimination and automated decision-making.

5.8.3 It is prohibited to use real personal data in training, fine-tuning, or evaluation of models without a declared and legitimate purpose and without de-identification, where the purpose permits it, applying the masking of INT-SEG-002 in non-production environments.

5.8.4 Processing by artificial intelligence that may generate high risk to data subjects — including automated decision-making with significant effect — requires a DPIA pursuant to POP-SEG-009 and Art. 38 of the LGPD, prior to deployment.

5.9 Use of Social Media

5.9.1 The use of social media is permitted for business functions, especially Marketing and Commercial, exclusively for corporate purposes. Publishing or processing confidential data or personal data through this channel is prohibited.

5.9.2 Personal use of social media on corporate resources is prohibited for all employees who do not hold a business function that justifies such use.

6. RESPONSIBILITIES

The Information Technology (IT) area is responsible for ensuring compliance with this policy across all areas and departments of the Organization.

6.1 Technology/Product Lead: Ensure that privacy requirements are integrated into the lifecycle of products and projects; secure resources and prioritization for their implementation; authorize entry into production only after verification of privacy requirements. Accountable for the dissemination and observance of this policy across the Organization's areas.

6.2 Data Protection Officer (DPO): Guide teams in defining privacy requirements; evaluate the Privacy by Design Questionnaire (FOR-17-001); assess the necessity of and validate DPIAs pursuant to POP-SEG-009; coordinate the post-deployment monitoring provided for in section 5.2.7; maintain the Record of Processing Activities (ROPA) updated in accordance with POL-SEG-029 and POL-SEG-027.

6.3 ISPC (Information Security and Privacy Committee): Evaluate, jointly with the DPO, the questionnaires and projects submitted; recommend adjustments, approve, or veto projects; deliberate on residual risks and approve this policy.

6.4 Information Security Lead: Define and validate technical controls for security, de-identification, masking, and disposal; verify adherence to this policy in ISMS evaluations and audits.

6.5 Development Teams: Implement the privacy requirements defined for each project or feature; apply masking in test environments; report to the DPO and the Information Security Lead any processing of personal data without a defined privacy requirement.

6.6 Reporting Channel: Any violation or suspected violation of this policy must be reported immediately. Violations related to privacy and personal data protection are reported to the Data Protection Officer (DPO) at dpo@px.center. Violations related to information security are reported to the Information Security area at security@px.center. Cases are investigated diligently and confidentially and, when confirmed, result in appropriate measures.

Non-compliance with this policy subjects the offender to the disciplinary measures set out in PX.Center's internal regulations, without prejudice to applicable legal sanctions.

7. RECORDS MANAGEMENT

Records arising from this policy include: completed and evaluated Privacy by Design questionnaires (FOR-17-001); privacy requirements documented in project artifacts; DPIAs prepared pursuant to POP-SEG-009; evidence of deletion, return, and disposal of personal data; records of masking in test environments; and records of the post-deployment monitoring provided for in section 5.2.7.

Questionnaires, DPIAs, and other evidence are stored in the ISMS document repository. Non-conformities related to this policy are recorded and addressed in the corporate non-conformity management tool, pursuant to POP-SGI-006. The ROPA is maintained by the DPO, in accordance with POL-SEG-029 and POL-SEG-027.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on the date of its publication and is valid for an indefinite period. Review occurs annually or upon relevant legislative, regulatory, or organizational change, subject to formal approval by the ISPC (Information Security and Privacy Committee).

9. ANNEXES

FOR-17-001: Privacy by Design and DPIA Questionnaire — instrument for surveying privacy requirements, completed by the requesting business unit and evaluated by the DPO and the ISPC, as provided in section 5.2.3. Other operational records referenced in this policy reside in the ISMS document repository (questionnaires, DPIAs, and evidence of deletion and return) and in the corporate non-conformity management tool (non-conformities).

CHANGE HISTORY

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