Privacy by Design and by Default Policy

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

Code:	*POL-SIP-028*
Responsible area:	*Privacy*
Issue date:	*24/06/2026*
Approval authority:	*DPO / CSIP*

1. PURPOSE/OBJECTIVE

This policy establishes mandatory guidelines for embedding privacy from conception (privacy by design) and privacy by default into all PX.Center products, systems, projects, and processes that involve the processing of 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 (LGPD), which mandates the observance of security and privacy measures from the product or service conception phase through to execution. This policy derives from the Information Security Policy (POL-SIP-001), to which it is subordinate.

2. SCOPE/APPLICABILITY

Applies to the entire lifecycle of PX.Center products, systems, applications, integrations, and business processes that process personal data, in situations where the Organisation acts as controller or as processor.

Covers the conception, development, testing, user acceptance testing, production, retention, return, and disposal phases, in on-premises environments and in 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 programmes, new applications, technologies, or services that process personal data. It includes artificial intelligence-based systems and features, insofar as they process personal data at any stage of their lifecycle.

Subordinate to the Information Security Policy (POL-SIP-001) and integrated into the Information Security Management System.

3. USERS/TARGET AUDIENCE

Technology/Product Leader, development and engineering teams, Information Security Leader, Data Protection Officer (DPO), Information Security and Privacy Committee (CSIP), project managers, and contracted third parties participating 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)
- Lei nº 13.709/2018 (LGPD), in particular Article 6 (principles of adequacy and necessity), Article 38 (Data Protection Impact Assessment), and Article 46, paragraph 2

- POL-SIP-001: Information Security Policy
- POL-SIP-029: Privacy and Personal Data Protection Policy
- POL-SIP-027: Privacy Governance Policy
- POL-SIP-005: Secure Disposal Policy
- POL-SIP-006: Cryptography Policy
- POL-SIP-007: Secure Development Policy
- POL-SIP-018: Testing and User Acceptance Testing Policy
- POP-SIP-009: Personal Data Protection Impact Assessment (RIPD)
- POP-SGI-006: Non-Conformity Treatment
- INT-SIP-018: Data Masking in Test Environments
- INN-RAD-009: Personal Data Protection
- MAN-SGI-001: SGI Manual
- FOR-17-001: Privacy by Design and RIPD 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 embedded 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 materialise. Technical measures apply, such as anonymisation or pseudonymisation, 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 embedded in products, systems, and services by default, requiring no action from the data subject. The data subject receives the product or service with all safeguards activated from the start of development, is informed of which data are collected and for which legitimate purpose, and is not required to take protective action to ensure their privacy.

5.1.3 Privacy embedded into design: privacy is an elementary component of the designed core functionality, not an add-on. Any data-subject data-sharing option starts restricted, and the options presented must not be biassed toward acceptance of sharing or automatic permission.

5.1.4 Full functionality: positive-sum, not zero-sum: embed privacy into technologies, processes, and systems without compromising their full functionality, accommodating non-privacy-related objectives in an additive manner, with documentation of the interests involved and pursuit of multifunctional solutions that eliminate the need to sacrifice legitimate objectives.

5.1.5 End-to-end security: protection throughout the entire lifecycle: adoption of robust security measures from the beginning through to the end of processing, ensuring the protection of personal data at all stages of its lifecycle.

5.1.6 Visibility and transparency: processing practices remain visible and verifiable, sustaining accountability and the trust of data subjects, 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 subjects' interests, through robust privacy standards, mechanisms for the exercise of their rights, facilitated access, and security measures that ensure the confidentiality, integrity, and availability of data throughout their entire lifecycle.

5.2 Privacy from conception (privacy by design)

5.2.1 It is mandatory to identify and record privacy requirements at the start 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 artefacts and follow the secure development lifecycle defined in POL-SIP-007. Cryptographic controls apply in accordance with POL-SIP-006.

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

5.2.4 A Personal Data Protection Impact Assessment (RIPD) is mandatory, pursuant to POP-SIP-009 and Article 38 of the LGPD, when processing may 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 assesses and records the decision regarding the need for a RIPD.

5.2.5 The DPO and CSIP may recommend adjustments, approve, or veto a project, even temporarily, after analysing the applicable risks and mitigation mechanisms.

5.2.6 It is prohibited to deploy to 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 processing personal data is monitored for development and performance. Post-deployment monitoring is carried out at least once a year and, whenever necessary, at shorter intervals, under the coordination of the DPO and CSIP, with a view to continuous improvement following the PDCA cycle.

5.3 Privacy by default

5.3.1 Every default configuration of a product, system, or feature must be the most privacy-restrictive option. Data sharing, profile visibility, and additional data collections remain disabled by default and depend on an affirmative action by the data subject.

5.3.2 Personal data collection is limited to the minimum necessary to fulfil 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 (Article 6, items II and III, of the LGPD).

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

5.4 Minimisation and de-identification

5.4.1 Development teams must anonymise or pseudonymise personal data when the purpose of processing allows, with priority given to anonymisation.

5.4.2 Pseudonymisation requires segregated storage of the additional information enabling 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 are retained only for the period necessary to fulfil the purpose of processing or a legal or regulatory obligation. Once the purpose has ended, it is mandatory to erase or anonymise the data, in accordance with control 7.4 of ISO/IEC 27701:2019.

5.5.2 Retention periods by personal data category 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 the media containing them follows the secure disposal procedures defined in POL-SIP-005, with a formal record of the erasure.

5.6 Return and erasure upon contract termination

5.6.1 In contracts where PX.Center acts as processor, it is mandatory, upon termination of the service provision, to return to the controller or erase the personal data processed, in accordance with documented instructions from the controller, in compliance with control 8.4 of ISO/IEC 27701:2019.

5.6.2 Erasure must be formally evidenced to the controller. Backup copies containing the data are subject to the same erasure regime at the end of their retention cycle.

5.6.3 Retention of data after contract termination is only permitted where required by a legal or regulatory obligation, 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 user acceptance testing environments without masking, applied in accordance with INT-SIP-018.

5.7.2 Testing and user acceptance testing environments observe the segregation and access controls defined in POL-SIP-018.

5.8 Artificial intelligence and Privacy by Design

5.8.1 Artificial intelligence-based systems, features, and agents that process personal data fully observe the seven principles of section 5.1 and the controls of 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 assessment must consider the legal basis, minimisation 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 the training, fine-tuning, or evaluation of models without a declared and legitimate purpose and without de-identification where the purpose permits, applying the masking of INT-SIP-018 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 RIPD pursuant to POP-SIP-009 and Article 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, particularly Marketing and Commercial, exclusively for corporate purposes; publication or processing of confidential data or personal data through this channel is prohibited.

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

6. RESPONSIBILITIES

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

6.1 Technology/Product Leader: ensure that privacy requirements are integrated into the lifecycle of products and projects; secure resources and prioritisation for their implementation; authorise go-live only after verification of privacy requirements. Responsible for the dissemination and compliance with this policy across the Organisation's areas.

6.2 Data Protection Officer (DPO): guide teams in defining privacy requirements; assess the Privacy by Design Questionnaire (FOR-17-001); evaluate the need for and validate RIPDs pursuant to POP-SIP-009; coordinate post-deployment monitoring as provided for in section 5.2.7; maintain the ROPA updated in accordance with POL-SIP-029 and POL-SIP-027.

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

6.4 Information Security Leader: define and validate technical security, de-identification, masking, and disposal controls; verify adherence to this policy during SGI assessments 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 Leader any processing of personal data without a defined privacy requirement.

6.6 Violations 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, give rise to 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 assessed Privacy by Design questionnaires (FOR-17-001); privacy requirements documented in project artefacts; RIPDs prepared pursuant to POP-SIP-009; evidence of erasure, return, and disposal of personal data; masking records in test environments; and post-deployment monitoring records as provided for in section 5.2.7.

Questionnaires, RIPDs, and other evidence are stored in the SGI 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-SIP-029 and POL-SIP-027.

8. VALIDITY / DOCUMENT MANAGEMENT

This policy enters into force on its publication date and remains valid indefinitely. Review takes place annually or upon relevant legislative, regulatory, or organisational change, subject to formal approval by the CSIP (Information Security and Privacy Committee).

9. ANNEXES

FOR-17-001: Privacy by Design and RIPD Questionnaire — a privacy requirements survey instrument completed by the requesting area and assessed by the DPO and CSIP, as provided for in section 5.2.3. The remaining operational records referenced in this policy reside in the SGI document repository (questionnaires, RIPDs, and erasure and return evidence) and in the corporate non-conformity management tool (non-conformities).

CHANGE HISTORY

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