Data Subject Rights Procedure

Reception, identity verification, triage, fulfillment, and logging of Data Subject Access Requests (DSARs) at PX.Center

Code	POP-SEG-008
Responsible Area	Privacy
Issue Date	June 24, 2026
Approval Authority	DPO / CSIP

1. OBJECTIVE

This procedure establishes the operational workflow for receiving, verifying the identity of, triaging, fulfilling, and recording Data Subject Access Requests (DSARs) directed to PX.Center, in compliance with Articles 18 and 20 of Law 13,709/2018 (Brazilian General Data Protection Law — LGPD) and in accordance with controls 7.3 (controller obligations toward data subjects) and 8.3 (processor support of controller obligations toward data subjects) of ISO/IEC 27701:2019.

The objective is to ensure that every request is registered, identity-verified, triaged, fulfilled within the statutory deadline of 15 business days, and documented in an auditable manner — guaranteeing the full exercise of rights provided under the LGPD and PX.Center's accountability obligations.

This procedure applies to all data subject requests received by PX.Center, both in situations where the organization acts as a controller and in situations where it acts as a processor of personal data. It covers all business units, systems, technology environments, and third-party relationships that process personal data, and supplements the guidelines of POL-SEG-029 (base standard for personal data processing) and POL-SEG-027 (privacy governance).

It is aligned with the Information Security Policy (POL-SEG-001), from which the applicable privacy guidelines derive.

2. DEPARTMENTS INVOLVED

- **Data Protection Officer (DPO):** Leads the fulfillment process, verifies the identity of the requester, performs triage, responds to the data subject within the deadline, formalizes denials with Legal, maintains the auditable record of all requests, and investigates violations of this procedure through the channel dpo@px.center.
- **Information Technology:** Executes personal data lookups in the systems under its management, applies the technical measures of anonymization, blocking, or erasure, and ensures that service channels adopt adequate security measures.
- **Information Security:** Receives, through security@px.center, violation communications that constitute a security incident and leads their treatment in accordance with POL-SEG-002.
- **Legal:** Supports the analysis of legal bases, the substantiation of denials, the evaluation of objections, and the verification of retention obligations.
- **Area Managers:** Provide the personal data processed within their areas of responsibility, respond to data-lookup requests within the timeframe set by the DPO, and keep their areas' Records of Processing Activities (ROPA) up to date.
- **Target Audience:** All employees and third parties who, in the exercise of their duties, receive, forward, or support the fulfillment of data subject requests on behalf of PX.Center.

3. ANNEXES / REFERENCES

There are no annexes.

4. DEFINITIONS

- **Data Subject:** The natural person to whom the personal data being processed relates.
- **Controller:** The natural or legal person responsible for decisions regarding the processing of personal data.
- **Processor:** The natural or legal person who processes personal data on behalf of the controller.
- **Data Protection Officer (DPO):** The person designated by the organization to act as the communication channel among PX.Center, data subjects, and the National Data Protection Authority (ANPD — Autoridade Nacional de Proteção de Dados).
- **Identity Verification:** The set of evidence proving that the requester is the data subject or their legally authorized representative.
- **Official Channel:** The mailbox dpo@px.center — the sole valid means for processing data subject requests.
- **DSAR:** Data Subject Access Request — a formal exercise of a right by the data subject.
- **Automated Decision:** A decision made solely on the basis of automated personal data processing, including personal, professional, consumer, and credit profiling.

5. PROCESS DESCRIPTION

5.1 Reception

Every data subject request, regardless of the channel through which it reaches the organization, must be directed to the official channel dpo@px.center and recorded with the date of receipt. It is the duty of every employee to immediately forward to the official channel any request received through any other means. Processing a request outside the official channel or without a corresponding record is prohibited.

5.2 Identity Verification

Responding to a request without prior confirmation of the requester's identity is prohibited. The DPO requests the elements necessary to prove that the requester is the data subject or their legal representative, observing the data minimization principle — no data more sensitive or in greater volume than originally collected may be required, and disproportionate obstacles to the exercise of rights may not be imposed.

1. **Accepted documents for proof:** National Driver's License (CNH), National Identity Card (RG), passport, or Brazilian tax ID (CPF) accompanied by a second document that enables cross-referencing of registration data. For low-risk requests — such as opting out of marketing communications — a request from an already-registered email address or phone number is considered sufficient.
2. **Legal representative:** When the request is submitted by a third party, proof of representative authority is required (power of attorney, guardianship, conservatorship, or equivalent document), along with identification of the representative themselves.

3. **Verification failure:** If the data subject does not respond to the request for additional information or if legitimacy cannot be confirmed, the request is rejected with formal justification to the requester.
4. **Retention of verification records:** Identity verification evidence is stored for 3 (three) years, corresponding to the statute of limitations, to protect the organization's rights in the event of a challenge by the data subject or in judicial, administrative, or arbitration proceedings. This data is used exclusively for verification purposes.

5.3 Triage

The DPO determines whether PX.Center acts as a controller or as a processor with respect to the data that is the subject of the request. When PX.Center acts as a processor, the request is forwarded to the client controller with a formal record of the referral — in compliance with control 8.3 of ISO/IEC 27701:2019 — within the timeframe defined in the contract or, in the absence of a specific contractual deadline, within 5 business days, so as to preserve the controller's response window to the data subject. When it is not possible to identify the responsible controller, the data subject is directed to submit the request directly to the controller, and the request is closed and archived. Pursuant to Article 18, §4, I, of the LGPD, if it is determined that PX.Center is not a processing agent for the data in question, the data subject is informed of this circumstance, with the indication of the responsible agent whenever possible.

5.4 Fulfillment

When PX.Center acts as a controller, the DPO consults the ROPA to identify the categories of the data subject's data and the processes that handle them, and conducts the data lookup in the organization's systems with support from Information Technology and the relevant area managers. The response to the data subject must be clear, written in accessible language, provided at no cost, and issued within 15 business days of receipt (LGPD, Art. 19), in accordance with POL-SEG-029. The following rights, provided for in Articles 18 and 20 of the LGPD, are fulfilled:

5.4.1 Confirmation of Processing

The DPO confirms or denies the existence of personal data processing relating to the data subject, indicating the origin of the data, any absence of a record, and the criteria and purpose of processing, subject to trade and industrial secrecy.

5.4.2 Access to Data

The DPO provides the data subject with a list of their personal data processed by the organization, via secure electronic means or, at the data subject's option, in printed form, omitting information protected by operational secrecy.

5.4.3 Correction of Incomplete, Inaccurate, or Outdated Data

The DPO forwards to the responsible departments the request to update or correct the data and, when the data has been shared with third parties, arranges for notification to those parties so they may replicate the correction.

5.4.4 Anonymization, Blocking, or Erasure of Unnecessary, Excessive, or Non-Compliant Data

The DPO, together with Information Technology, assesses the technical conditions and the existence of a legal basis for preserving the data, and determines the appropriate anonymization, temporary blocking, or erasure, including in backups where applicable.

5.4.5 Data Portability

The DPO provides the data in a structured format, in common language and an open format (e.g., XML), so that it may be transmitted to another controller, subject to trade and industrial secrecy.

5.4.6 Information on Data Sharing with Public and Private Entities

The DPO expressly names the public and private entities with which the organization has shared the data subject's data.

5.4.7 Erasure of Data Processed with Consent

Once consent is withdrawn, the DPO orders the erasure of data processed under that legal basis, except as provided in Article 16 of the LGPD — in which cases the impossibility is communicated and justified to the data subject.

5.4.8 Revocation of Consent

The DPO processes revocation free of charge and at any time, ratifying the processing already carried out under the previous consent. The organization may retain the data where another legal basis supports the processing.

5.4.9 Right to Be Informed of the Option Not to Consent and the Consequences of Refusal (Art. 18, VII, LGPD)

The DPO informs the data subject, clearly, expressly, and unequivocally, that they may withhold consent to a particular processing activity and what the consequences of that refusal are. As a general rule, this information is included in the Privacy Notice and, where the specific case requires it, is provided individually in response to the request.

5.4.10 Objection to Processing (Art. 18, IX, LGPD)

When processing is based on a legal basis other than consent and the data subject objects to processing carried out in non-compliance with the LGPD, the DPO — with support from Legal — analyzes the objection, verifies the legitimacy of the legal basis invoked by the organization, and, depending on the outcome, either ceases the contested processing or substantiates its continuation, communicating the decision to the data subject.

5.4.11 Review of Automated Decisions (Art. 20, LGPD)

A data subject may request the review of decisions made solely on the basis of automated personal data processing that affects their interests, including decisions on personal, professional, consumer, and credit profiling. The DPO — with support from the area responsible for the decision — provides clear and adequate information about the criteria and procedures used in the automated decision,

subject to operational secrecy, and forwards the review request for re-analysis, communicating the outcome to the data subject.

5.5 Substantiated Denial

When a legal basis prevents the total or partial fulfillment of a request — for example, compliance with a legal obligation (Art. 7, II) or the regular exercise of rights (Art. 7, VI) — the DPO, with support from Legal, issues a substantiated denial to the data subject, expressly indicating the applicable legal basis. A denial without documented substantiation is prohibited.

5.6 Per-Right Log (Fulfillment Log)

Every request generates an individual auditable record maintained by the DPO in the privacy management tool, containing at minimum: (a) the type of right requested (among the rights listed in items 5.4.1 through 5.4.11); (b) the date the request was opened; (c) the date the response was sent to the data subject; (d) the outcome of the fulfillment (fulfilled, partially fulfilled, denied, or forwarded to the controller); (e) the person responsible for the fulfillment; (f) evidence of identity verification, the content of the request, the triage performed, the response or referral issued, and proof of compliance with the deadline. The record preserves the complete history of the request — correspondence exchanged, decisions made and their rationale, and copies of the information provided to the data subject — for accountability and legal protection purposes.

5.7 Coordination with Incident Management

When a data subject request reveals, or stems from, a security incident involving personal data, the DPO triggers the incident management process in accordance with POL-SEG-002, observing the 72 (seventy-two) hour notification deadline to the National Data Protection Authority (ANPD) and to affected data subjects where applicable, without prejudice to the continuation of request fulfillment within the 15 business-day period.

5.9 Compliance and Consequences of Violations

Any and all violations of this procedure must be reported immediately to the Data Protection Officer (DPO) — the party responsible for investigating procedural violations — through the channel dpo@px.center. When the violation involves a security incident, it must also be reported to Information Security through security@px.center, for treatment in accordance with POL-SEG-002. Every suspected violation is investigated diligently and confidentially and, once confirmed, results in appropriate measures, including disciplinary action, pursuant to PX.Center's internal regulations and applicable legal and contractual provisions.

6. PROCESS FLOWS

Flow A — Direct Data Subject (PX.Center as Controller): Data subject submits request to dpo@px.center, or the request is redirected to the official channel → DPO records the request with the opening date and type of right → DPO verifies the identity of the requester (item 5.2) → Information Technology and area managers perform the data lookup in the systems based on the ROPA → DPO issues a clear and accessible response within the deadline set by POL-SEG-029 → DPO completes the fulfillment record (item 5.6).

Flow B — Request Involving a Client (PX.Center as Processor): Request received from the data subject or the client is recorded by the DPO → DPO identifies the client controller for the data in question → DPO forwards the request to the controller with a formal record within the timeframe in item 5.3 → PX.Center provides support to the controller in the data lookup and fulfillment execution, when contractually provided, in accordance with control 8.3 of ISO/IEC 27701:2019.
Flow C — Substantiated Denial: DPO identifies a legal basis that prevents total or partial fulfillment → Legal validates the substantiation and applicable legal basis → DPO communicates the denial to the data subject within the deadline, expressly indicating the legal basis → DPO records the denial and its grounds.
Flow D — Review of Automated Decision: DPO records the request and verifies the identity of the requester → DPO, together with the area responsible for the decision, identifies the criteria and procedures of the automated decision → The decision is reviewed and the data subject receives clear information about the criteria applied, subject to operational secrecy → DPO communicates the outcome of the review and records the fulfillment.

7. QUALITY

Indicators:

- 100% of requests responded to within 15 business days.
- 100% of responses preceded by identity verification of the requester.
- Complete and intact records for 100% of requests received, including per-right logs, referrals, and denials.

The DPO monitors these indicators and reports deviations to the CSIP in monthly meetings. Non-conformities identified in the process are recorded in the corporate non-conformity management tool and treated in accordance with POP-SGI-006.

Records Management: Fulfillment records, per-right logs, and identity verification evidence reside in the privacy management tool under DPO custody, with identity evidence retained for 3 years (item 5.2.d); the ROPA remains under DPO custody; process non-conformities are recorded in the corporate non-conformity management tool. It is mandatory to preserve the integrity of records, with access restricted by need-to-know, and to keep them available for internal and external ISMS audits.

Validity: This procedure enters into force on the date of publication, with validity for an indefinite period, and is reviewed annually from the date of approval or at any time in the event of a material change in legislation, ANPD guidance, organizational structure, or processing activities.

CHANGE HISTORY

Version	Date	Author	Description
00	Apr 1, 2026	SGI	Document creation
01	Jun 24, 2026	SGI	Recoding to acronym-based numbering