Data Subject Rights Fulfillment Procedure

Receipt, identity verification, triage, fulfillment, and logging of data subject requests (DSAR) at PX.Center.

Code:	*POP-SIP-008*
Responsible area:	*Privacy*
Issue date:	*24/06/2026*
Approval authority:	*DPO / CSIP*

1. OBJECTIVE

Establish the operational workflow for receiving, verifying the identity of, triaging, fulfilling, and recording data subject requests (Data Subject Access Requests — DSAR) submitted to PX.Center, in compliance with art. 18 and art. 20 of Law 13.709/2018 (LGPD) and in conformity with controls 7.3 (controller obligations toward data subjects) and 8.3 (processor support for controller obligations toward data subjects) of ISO/IEC 27701:2019.

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

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

In alignment with the Information Security Policy (POL-SIP-001), from which the applicable privacy guidelines are derived.

2. DEPARTMENTS INVOLVED

Data Protection Officer (DPO): leads fulfillment, verifies the requester's identity, performs triage, responds to the data subject within the deadline, formalizes denials with Legal, maintains an auditable record of all requests, and investigates violations of this procedure via the channel dpo@px.center.

Information Technology: carries out the collection of personal data in systems under its management, applies technical measures for anonymization, blocking, or deletion, and ensures that fulfillment channels adopt appropriate security measures.

Information Security: receives, via the channel security@px.center, violation notifications that constitute a security incident, and manages their handling in accordance with POL-SIP-002.

Legal: supports the analysis of legal grounds, the substantiation of denials, the assessment of objections, and the verification of retention obligations.

Area managers: provide the personal data processed in the processes under their responsibility, respond to data-collection requests within the deadline defined by the DPO, and keep the ROPA for their processes 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

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 appointed by the organization to act as a communication channel between PX.Center, data subjects, and the National Data Protection Authority (ANPD).

Identity verification: the set of evidence that proves the requester is the data subject or their duly appointed legal representative.

Official channel: the dpo@px.center mailbox, the sole valid means for processing data subject requests.

DSAR: Data Subject Access Request — a formal request by a data subject to exercise a right.

Automated decision: a decision made solely on the basis of automated processing of personal data, including profiling of personal, professional, consumer, and credit characteristics.

5. PROCESS DESCRIPTION

5.1 Receipt. 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 logged 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 log entry 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 verify that the requester is the data subject or their legal representative, observing the minimization principle — data more sensitive or in greater volume than originally collected may not be required, nor may disproportionate barriers to the exercise of rights be imposed.

a) Accepted documents for verification: National Driver's License (CNH), National Identity Card (RG), passport, or CPF accompanied by a second document enabling cross-referencing of registration data. For low-risk requests, such as marketing communications opt-out, a request submitted from a registered email address or phone number is considered sufficient.

b) Legal representative: when the request is submitted by a third party, proof of representative authority is required (power of attorney, guardianship, curatorship, or equivalent document), along with the identification of the representative themselves.

c) Verification failure: if the data subject does not respond to the request for additional information or their legitimacy cannot be verified, the request is rejected with formal justification provided to the requester.

d) Retention of verification records: identity verification evidence is retained 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. These data are used exclusively for verification purposes.

5.3 Triage. The DPO determines whether PX.Center acts as a controller or 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 deadline specified 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 art. 18, § 4º, 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 accordingly, with the identification of the relevant agent provided 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-collection exercise across 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 free of charge, and issued within 15 business days of receipt (LGPD, art. 19), in accordance with POL-SIP-029. The rights listed below, as provided for in art. 18 and art. 20 of the LGPD, are fulfilled.

5.4.1 Confirmation of the existence of processing. The DPO confirms, affirmatively or negatively, the existence of processing of the data subject's personal data, indicating the origin of the data, any absence of records, and the criteria and purposes of the processing, subject to commercial and industrial trade secrets.

5.4.2 Access to data. The DPO provides the data subject with the list of their personal data processed by the organization, via a secure electronic means or, at the data subject's discretion, in printed form, omitting information protected by business confidentiality.

5.4.3 Correction of incomplete, inaccurate, or outdated data. The DPO forwards the update or rectification of data to the responsible areas and, when data has been shared with third parties, arranges for notification of those parties to replicate the correction.

5.4.4 Anonymization, blocking, or deletion of unnecessary, excessive, or non-LGPD-compliant data. The DPO assesses, with Information Technology, the technical conditions and the existence of a legal basis for retaining the data, and determines the applicable anonymization, temporary blocking, or deletion, including in backups where applicable.

5.4.5 Data portability. The DPO provides the data in structured, commonly used, and open format (e.g., XML), so that it may be transmitted to another controller, subject to commercial and industrial trade secrets.

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 engaged in shared use of the data subject's data.

5.4.7 Deletion of data processed under consent. Upon withdrawal of consent, the DPO orders the deletion of data processed on that legal basis, except as provided in art. 16 of the LGPD; in such cases, the impossibility of deletion is communicated and justified to the data subject.

5.4.8 Withdrawal of consent. The DPO processes the withdrawal free of charge and at any time, with processing carried out under the prior consent remaining valid. The organization may retain the data where another legal basis supports continued processing.

5.4.9 Information on the possibility of withholding consent and on the consequences of refusal (art. 18, VII, of the LGPD). The DPO informs the data subject, in a clear, express, and unequivocal manner, that they may withhold consent for a given processing activity and what the consequences of such refusal are. As a rule, this information is included in the Privacy Notice and, where the specific circumstances require, is provided on a case-by-case basis in response to the request.

5.4.10 Objection to processing (art. 18, IX, of the LGPD). When processing is based on a legal ground other than consent and the data subject objects to processing carried out in violation of the LGPD, the DPO, with support from Legal, reviews the objection, verifies the legitimacy of the legal basis invoked by the organization, and either ceases the challenged processing or substantiates its continuation, communicating the decision to the data subject.

5.4.11 Review of automated decisions (art. 20 of the LGPD). The data subject may request a review of decisions made solely on the basis of automated processing of personal data that affect their interests, including profiling decisions of a personal, professional, consumer, or credit nature. 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 business trade secrets, and forwards the review request for re-examination, communicating the outcome to the data subject.

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

5.6 Per-right log (fulfillment record). Every request generates an individual auditable record, maintained by the DPO in the privacy management tool, containing at minimum: a) type of right requested (among the rights in items 5.4.1 through 5.4.11); b) date the request was opened; c) date of response to the data subject; d) outcome of fulfillment (fulfilled, partially fulfilled, denied, or forwarded to the controller); e) person responsible for fulfillment; f) evidence of identity verification, content of the request, triage performed, 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 information sent 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 activates the incident management process in accordance with POL-SIP-002, observing the 72 (seventy-two) hour notification deadline to the

National Data Protection Authority and to affected data subjects where applicable, without prejudice to the continued fulfillment of the request within the 15 business-day deadline.

5.9 Compliance and consequences of procedure violations. Any and all violations of this procedure must be reported immediately to the Data Protection Officer (DPO), responsible for investigating procedure violations, via the channel dpo@px.center. When the violation involves an information security incident, it must also be reported to the Information Security department via the channel security@px.center, for handling in accordance with POL-SIP-002. Every suspected violation is investigated diligently and confidentially and, once confirmed, gives rise to appropriate measures, including disciplinary action, pursuant to PX.Center's internal policies and applicable legal and contractual provisions.

6. PROCESS FLOW

Flow A — direct data subject (PX.Center as controller): the data subject submits a request to dpo@px.center, or the request is redirected to the official channel; the DPO logs the request with the opening date and type of right; the DPO verifies the requester's identity (item 5.2); Information Technology and area managers carry out the data-collection exercise in the systems based on the ROPA; the DPO issues a clear and accessible response within the deadline set by POL-SIP-029; the DPO completes the fulfillment record (item 5.6).

Flow B — request involving a client (PX.Center as processor): the request received from the data subject or the client is logged by the DPO; the DPO identifies the client controller of the data in question; the DPO forwards the request to the controller with a formal record, within the deadline in item 5.3; PX.Center provides support to the controller in the data-collection exercise and the execution of the response, where contractually stipulated, in accordance with control 8.3 of ISO/IEC 27701:2019.

7.

Flow C — substantiated denial: the DPO identifies a legal ground that prevents total or partial fulfillment; Legal validates the substantiation and the applicable legal basis; the DPO communicates the denial to the data subject within the deadline, expressly stating the legal basis; the DPO records the denial and its grounds.

Flow D — automated decision review: the DPO logs the request and verifies the requester's identity; the DPO, together with the area responsible for the decision, identifies the criteria and procedures of the automated decision; the decision is re-examined and the data subject receives clear information about the criteria applied, subject to business trade secrets; the DPO communicates the outcome of the review and records the fulfillment.

		QUALITY	**Indicators: 100% of requests responded to within 15 business days; 100% of responses preceded by identity verification of the requester; complete logging of 100% of requests received, including per-right logs, referrals, and denials.**
	The DPO monitors the indicators and reports deviations to the CSIP at the monthly meeting. Non-conformities identified in the process are recorded in the corporate non-conformity management tool and handled in accordance with POP-SGI-006.		Records management: fulfillment records for data subjects, per-right logs, and identity verification evidence reside in the privacy management tool, under the custody of the DPO, with identity evidence retained for 3 years (item 5.2.d); the ROPA remains under the DPO's 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 on a need-to-know basis, and

			to keep them available for internal and external SGI audits.
	Validity: this procedure takes effect on the date of its publication, remains valid for an indefinite period, and is reviewed annually from the date of approval or at any time in response to a material change in legislation, ANPD guidance, organizational structure, or processing activities.		CHANGE HISTORY