Privacy Requirements Catalog

Introduction

This document serves as a catalog of privacy requirements aligned with the General Data Protection Regulation (GDPR), the Spanish Organic Law on Personal Data Protection and Digital Rights Guarantee (LOPDGDD), the National Security Scheme (ENS), ISO/IEC 27001, and IEEE 29148. It aims to provide a structured and actionable guide for technical, legal, and auditing teams to ensure compliance and integrate privacy by design in technological systems.

Categories of Privacy Requirements

1. User Consent Management
2. User Rights
3. Data Minimization and Retention
4. Security Measures
5. International Data Transfers
6. Privacy by Design and Default

List of Privacy Requirements

1. User Consent Management

Requirement ID: PRIV-001
Title: Explicit Consent Acquisition
Description: Users' explicit consent must be obtained before processing personal data, as per GDPR Article 6. The consent should be freely given, informed, specific, and unambiguous.
Acceptance Criteria:

- Consent request includes an explicit checkbox (not pre-selected).
- A timestamped log of user consent is maintained.
  Priority: High
  Source: GDPR Article 6, LOPDGDD Article 6

Requirement ID: PRIV-002
Title: Withdrawal of Consent
Description: Users must be able to withdraw their consent at any time, and the withdrawal should be as easy as granting consent.
Acceptance Criteria:

- A clear and accessible mechanism for consent withdrawal.

- Immediate effect on processing upon withdrawal.
  Priority: High
  Source: GDPR Article 7

2. User Rights

Requirement ID: PRIV-003
Title: Right of Access
Description: Users must have the right to access their personal data and obtain a copy upon request. The system should provide an interface for this purpose.
Acceptance Criteria:

- User interface for access requests.
- Data provided within 30 days.
  Priority: High
  Source: GDPR Article 15, LOPDGDD Article 13

Requirement ID: PRIV-004
Title: Right to Erasure (Right to be Forgotten)
Description: Users must be able to request the deletion of their personal data when it is no longer necessary for the original purpose or if they withdraw consent.
Acceptance Criteria:

- Verification of eligibility for deletion.
- Secure deletion of data.
  Priority: High
  Source: GDPR Article 17, LOPDGDD Article 15

3. Data Minimization and Retention

Requirement ID: PRIV-005
Title: Data Minimization
Description: The system should collect only the minimum necessary personal data required for the intended purpose.
Acceptance Criteria:

- Review of required fields before data collection.
- Justification for each data field collected.
  Priority: Medium
  Source: GDPR Article 5(1)(c)

Requirement ID: PRIV-006
Title: Data Retention Policy
Description: Personal data should only be retained for as long as necessary. A retention policy should be in place.
Acceptance Criteria:

- Defined retention periods for different data types.

- Automatic deletion mechanisms.
  Priority: High
  Source: GDPR Article 5(1)(e), LOPDGDD Article 32

4. Security Measures

Requirement ID: PRIV-007
Title: Secure Data Storage
Description: Personal data must be stored securely using encryption and access controls.
Acceptance Criteria:

- Data encryption with approved standards.
- Role-based access control implementation.
  Priority: High
  Source: GDPR Article 32, ISO/IEC 27001

Requirement ID: PRIV-008
Title: Data Breach Notification
Description: Organizations must notify the data protection authority and affected users in case of a data breach.
Acceptance Criteria:

- Incident response plan in place.
- Notification sent within 72 hours of detection.
  Priority: High
  Source: GDPR Article 33, ENS Article 25

5. International Data Transfers

Requirement ID: PRIV-009
Title: Compliance for International Transfers
Description: Personal data should only be transferred outside the EU if the recipient country ensures adequate protection or appropriate safeguards are in place.
Acceptance Criteria:

- Verification of adequacy decision or standard contractual clauses.
- Documentation of transfer agreements.
  Priority: High
  Source: GDPR Article 44

6. Privacy by Design and Default

Requirement ID: PRIV-010
Title: Privacy by Design Implementation
Description: Privacy considerations should be integrated into the development lifecycle of products and services.
Acceptance Criteria:

- Privacy impact assessment conducted for new systems.
- Privacy-preserving techniques incorporated in development.
  Priority: High
  Source: GDPR Article 25, IEEE 29148