Privacy Policy Template

Document Control Information

- **Document Title:** Privacy Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Privacy Policy establishes [ORGANIZATION NAME]'s requirements for collecting, processing, storing, sharing, and protecting personal data in accordance with ISO 27001:2022 requirements and applicable privacy regulations. It provides a framework for ensuring that personal data is handled lawfully, fairly, and transparently.

1.2 Scope

This policy applies to: - All personal data processed by [ORGANIZATION NAME] - All forms of personal data, whether electronic or physical - All employees, contractors, consultants, and third parties who process personal data on behalf of [ORGANIZATION NAME] - All systems, applications, and processes that involve personal data - All locations where [ORGANIZATION NAME] operates

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Processing personal data lawfully, fairly, and transparently - Collecting personal data only for specified, explicit, and legitimate purposes - Minimizing personal data collection to what is necessary - Ensuring personal data accuracy and keeping it up to date - Retaining personal data only as long as necessary - Protecting personal data against unauthorized access, loss, or damage - Respecting individuals' rights regarding their personal data - Complying with applicable privacy laws and regulations

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

2. Definitions

2.1 Personal Data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

2.2 Special Categories of Personal Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

2.3 Data Processing

Any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.4 Data Controller

The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

2.5 Data Processor

A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

2.6 Data Subject

An identified or identifiable natural person to whom the personal data relates.

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

3. Privacy Principles

3.1 Lawfulness, Fairness, and Transparency

- Personal data shall be processed lawfully, fairly, and transparently
- A valid legal basis shall be identified for all processing activities
- Data subjects shall be informed about how their data is processed
- Privacy notices shall be clear, concise, and easily accessible
- Processing activities shall be documented and maintained

3.2 Purpose Limitation

- Personal data shall be collected for specified, explicit, and legitimate purposes
- Personal data shall not be processed in ways incompatible with those purposes
- Purpose changes shall be documented and communicated to data subjects
- New purposes shall have a valid legal basis
- Purpose compatibility shall be assessed before repurposing data

3.3 Data Minimization

- Personal data shall be adequate, relevant, and limited to what is necessary
- Only necessary data fields shall be collected
- Unnecessary data shall not be requested or stored
- Data collection forms shall be reviewed to ensure minimization
- Existing data shall be reviewed periodically for minimization

3.4 Accuracy

- Personal data shall be accurate and kept up to date
- Reasonable steps shall be taken to ensure accuracy
- Inaccurate data shall be rectified or erased promptly
- Data accuracy shall be verified at collection points
- Data subjects shall be able to request corrections

3.5 Storage Limitation

- Personal data shall be kept in a form that permits identification for no longer than necessary
- Retention periods shall be defined for all personal data
- Data shall be securely deleted when no longer needed
- Retention periods shall be documented and enforced
- Exceptions for archiving, research, or statistical purposes shall be documented

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

3.6 Integrity and Confidentiality

- Personal data shall be processed securely
- Appropriate technical and organizational measures shall be implemented
- Protection against unauthorized or unlawful processing shall be ensured
- Protection against accidental loss, destruction, or damage shall be ensured
- Security measures shall be regularly reviewed and updated

3.7 Accountability

- Responsibility for compliance shall be assigned
- Compliance shall be demonstrated through documentation
- Privacy impact assessments shall be conducted when appropriate
- Staff shall be trained on privacy requirements
- Compliance shall be regularly monitored and reviewed

4. Legal Basis for Processing

4.1 Valid Legal Bases

Personal data shall only be processed when one of the following legal bases applies: - Consent of the data subject - Necessary for the performance of a contract - Necessary for compliance with a legal obligation - Necessary to protect vital interests of the data subject or another person - Necessary for the performance of a task carried out in the public interest - Necessary for legitimate interests pursued by the controller or a third party

4.2 Consent Management

- Consent shall be freely given, specific, informed, and unambiguous
- Consent shall be obtained through a clear affirmative action
- Consent shall be documented and stored
- Consent shall be as easy to withdraw as to give
- Consent shall be regularly reviewed and refreshed if necessary
- Consent shall not be bundled with other matters
- Consent shall not be a precondition for services unless necessary

4.3 Legitimate Interests

- Legitimate interest assessments shall be conducted and documented
- Assessments shall consider:
    - Purpose of processing
    - Necessity of processing

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

    - Balance with data subject interests and rights
- Data subjects shall be informed of legitimate interests
- Objections to processing based on legitimate interests shall be addressed
- Legitimate interest assessments shall be regularly reviewed

5. Data Subject Rights

5.1 Right to Information

- Data subjects shall be informed about the processing of their personal data
- Information shall be provided in a concise, transparent, intelligible, and easily accessible form
- Information shall include:
    - Identity and contact details of the controller
    - Purposes and legal basis for processing
    - Recipients or categories of recipients
    - Retention periods
    - Data subject rights
    - Right to withdraw consent
    - Right to lodge a complaint
    - Source of data (if not collected directly)
- Information shall be provided at the time of data collection or within a reasonable period

5.2 Right of Access

- Data subjects shall have the right to obtain confirmation of processing
- Data subjects shall have the right to access their personal data
- Access requests shall be fulfilled without undue delay
- Access shall include:
    - Purposes of processing
    - Categories of personal data
    - Recipients or categories of recipients
    - Retention period
    - Information on other rights
    - Source of data (if not collected directly)
- Identity verification shall be performed before providing access
- Access shall be provided in a commonly used electronic format

5.3 Right to Rectification

- Data subjects shall have the right to rectify inaccurate personal data
- Data subjects shall have the right to complete incomplete personal data

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Rectification requests shall be fulfilled without undue delay
- Recipients of the data shall be informed of rectifications
- Rectification shall be documented
- Reasons for refusing rectification shall be explained to data subjects

5.4 Right to Erasure

- Data subjects shall have the right to erasure of personal data in specific circumstances
- Erasure requests shall be fulfilled without undue delay when applicable
- Circumstances for erasure include:
    - Data no longer necessary for original purposes
    - Withdrawal of consent
    - Successful objection to processing
    - Unlawful processing
    - Legal obligation to erase
- Exceptions to erasure shall be documented and explained
- Recipients of the data shall be informed of erasure
- Erasure shall be documented

5.5 Right to Restriction of Processing

- Data subjects shall have the right to restrict processing in specific circumstances
- Restriction requests shall be fulfilled without undue delay when applicable
- Circumstances for restriction include:
    - Contested accuracy
    - Unlawful processing where erasure is not requested
    - Data no longer needed but required by data subject for legal claims
    - Pending verification of overriding legitimate grounds
- Restricted data shall only be processed with consent or for specific exceptions
- Data subjects shall be informed before restrictions are lifted
- Recipients of the data shall be informed of restrictions

5.6 Right to Data Portability

- Data subjects shall have the right to receive their personal data in a structured, commonly used, and machine-readable format
- Data subjects shall have the right to transmit their data to another controller
- Portability applies to:
    - Data provided by the data subject
    - Processing based on consent or contract
    - Automated processing

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Portability requests shall be fulfilled without undue delay
- Portability shall not adversely affect the rights of others
- Technical feasibility of direct transmission shall be assessed

5.7 Right to Object

- Data subjects shall have the right to object to processing in specific circumstances
- Objection applies to processing based on:
    - Legitimate interests
    - Public interest tasks
    - Direct marketing
- Processing shall cease upon objection unless compelling legitimate grounds exist
- Objections to direct marketing shall always be honored
- Data subjects shall be explicitly informed of their right to object
- Objections shall be addressed without undue delay

5.8 Rights Related to Automated Decision Making

- Data subjects shall have the right not to be subject to purely automated decisions with significant effects
- Exceptions include:
    - Necessary for contract
    - Authorized by law
    - Based on explicit consent
- Safeguards shall be implemented for exceptions
- Data subjects shall have the right to:
    - Obtain human intervention
    - Express their point of view
    - Contest the decision
- Automated decision-making processes shall be regularly reviewed

6. Privacy by Design and Default

6.1 Privacy by Design

- Privacy shall be considered from the initial design stages
- Privacy requirements shall be integrated into systems and processes
- Privacy impact assessments shall be conducted for new systems and processes
- Technical and organizational measures shall be implemented to ensure privacy
- Privacy-enhancing technologies shall be considered and implemented where appropriate

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Systems and processes shall be designed to minimize personal data use
- Privacy design decisions shall be documented

6.2 Privacy by Default

- Default settings shall be privacy-protective
- Only necessary personal data shall be processed by default
- Data access shall be limited by default
- Data retention shall be limited by default
- Data sharing shall be limited by default
- Privacy-protective defaults shall be documented
- Default settings shall be regularly reviewed

6.3 Data Protection Impact Assessment

- Data Protection Impact Assessments (DPIAs) shall be conducted for high-risk processing
- High-risk processing includes:
  - Systematic and extensive profiling with significant effects
  - Large-scale processing of special categories of data
  - Systematic monitoring of publicly accessible areas
- DPIAs shall include:
  - Description of processing operations
  - Assessment of necessity and proportionality
  - Assessment of risks to data subjects
  - Measures to address risks
- DPIAs shall be conducted before processing begins
- DPIAs shall be reviewed when processing changes
- DPIA results shall be integrated into processing activities

7. Data Security

7.1 Security Measures

- Appropriate technical and organizational measures shall be implemented
- Measures shall ensure a level of security appropriate to the risk
- Measures may include:
  - Pseudonymization and encryption
  - Confidentiality, integrity, availability, and resilience
  - Restoration of availability and access after incidents
  - Regular testing and evaluation of effectiveness
- Security measures shall be documented
- Security measures shall be regularly reviewed and updated

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Security incidents shall be promptly addressed

7.2 Access Control

- Access to personal data shall be restricted to authorized personnel
- Access rights shall be based on job requirements
- Access shall be granted on a need-to-know basis
- Authentication mechanisms shall be implemented
- Access shall be logged and monitored
- Access rights shall be regularly reviewed
- Access shall be promptly revoked when no longer needed

7.3 Data Breach Management

- Data breach detection mechanisms shall be implemented
- Data breaches shall be reported internally without undue delay
- Data breaches shall be documented
- Data breaches shall be investigated
- Data breach notification to authorities shall be made within required timeframes
- Data breach notification to data subjects shall be made when required
- Remedial actions shall be implemented
- Lessons learned shall be incorporated into security measures

8. Data Transfers

8.1 Internal Transfers

- Internal transfers of personal data shall be documented
- Transfers shall have a valid legal basis
- Security during transfer shall be ensured
- Transfer necessity shall be assessed
- Transfer minimization shall be applied
- Transfer records shall be maintained
- Transfer security shall be regularly reviewed

8.2 Third-Party Transfers

- Third-party transfers shall be documented
- Transfers shall have a valid legal basis
- Data processing agreements shall be in place
- Third-party security shall be assessed
- Transfer necessity shall be assessed

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Transfer minimization shall be applied
- Transfer records shall be maintained
- Third-party compliance shall be regularly verified

8.3 International Transfers

- International transfers shall be documented
- Transfers shall only occur with adequate protection
- Protection mechanisms may include:
  - Adequacy decisions
  - Appropriate safeguards
  - Binding corporate rules
  - Standard contractual clauses
  - Explicit consent
  - Necessary for contract performance
  - Public interest
- Transfer necessity shall be assessed
- Transfer records shall be maintained
- International transfer mechanisms shall be regularly reviewed

9. Data Processors

9.1 Processor Selection

- Processors shall be selected based on sufficient guarantees
- Processor security capabilities shall be assessed
- Processor privacy practices shall be evaluated
- Processor compliance with regulations shall be verified
- Processor selection shall be documented
- Processor risks shall be assessed
- Processor selection shall be regularly reviewed

9.2 Processor Agreements

- Written agreements shall be established with processors
- Agreements shall include:
  - Processing only on documented instructions
  - Confidentiality commitments
  - Security measures
  - Sub-processor requirements
  - Data subject rights assistance
  - Breach notification requirements
  - Deletion or return of data

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

    - Compliance demonstration
    - Audit rights
- Agreements shall be reviewed by legal and privacy experts
- Agreements shall be regularly reviewed and updated

9.3 Processor Monitoring

- Processor compliance shall be regularly monitored
- Monitoring may include:
    - Self-assessments
    - Compliance reports
    - Certifications
    - Audits
- Non-compliance shall be addressed promptly
- Monitoring results shall be documented
- Monitoring frequency shall be based on risk
- Monitoring effectiveness shall be regularly assessed

10. Records of Processing Activities

10.1 Processing Records

- Records of processing activities shall be maintained
- Records shall include:
    - Controller contact details
    - Purposes of processing
    - Categories of data subjects and personal data
    - Categories of recipients
    - International transfers
    - Retention periods
    - Security measures
- Records shall be in written form, including electronic form
- Records shall be made available to supervisory authorities upon request
- Records shall be regularly reviewed and updated
- Record accuracy shall be verified

10.2 Processing Inventory

- A comprehensive inventory of processing activities shall be maintained
- The inventory shall be centrally managed
- The inventory shall be regularly updated
- The inventory shall be used for compliance verification
- The inventory shall support risk assessments

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- The inventory shall be accessible to relevant personnel
- The inventory shall be protected from unauthorized access

11. Training and Awareness

11.1 Privacy Training

- All staff shall receive privacy training
- Training shall be provided at onboarding and regularly thereafter
- Training shall cover:
    - Privacy principles
    - Legal requirements
    - Organizational policies and procedures
    - Data subject rights
    - Security measures
    - Breach reporting
    - Individual responsibilities
- Training shall be role-specific where appropriate
- Training completion shall be documented
- Training effectiveness shall be assessed
- Training materials shall be regularly updated

11.2 Privacy Awareness

- Privacy awareness shall be promoted throughout the organization
- Awareness activities may include:
    - Communications
    - Newsletters
    - Posters
    - Intranet resources
    - Team discussions
- Awareness shall address current privacy topics and risks
- Awareness effectiveness shall be assessed
- Awareness materials shall be regularly updated
- Awareness shall be integrated into organizational culture

12. Compliance and Audit

12.1 Compliance Monitoring

- Privacy compliance shall be regularly monitored

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Monitoring shall cover:
  - Policy implementation
  - Procedure adherence
  - Control effectiveness
  - Risk management
  - Incident response
- Monitoring results shall be documented
- Non-compliance shall be addressed
- Monitoring methods shall be regularly reviewed
- Monitoring effectiveness shall be assessed

12.2 Privacy Audits

- Regular privacy audits shall be conducted
- Audits shall be conducted by qualified personnel
- Audit scope shall be clearly defined
- Audit findings shall be documented
- Remediation plans shall be developed for findings
- Remediation progress shall be tracked
- Audit results shall be reported to management
- Audit program shall be regularly reviewed

12.3 Continuous Improvement

- Privacy practices shall be continuously improved
- Improvement sources include:
  - Audit findings
  - Monitoring results
  - Incident lessons learned
  - Regulatory changes
  - Technology developments
  - Stakeholder feedback
- Improvements shall be prioritized based on risk
- Improvement implementation shall be tracked
- Improvement effectiveness shall be assessed
- Improvement opportunities shall be regularly identified

13. Roles and Responsibilities

13.1 Management

- Approve privacy policies
- Provide resources for privacy program

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Review privacy performance
- Address significant privacy issues
- Support privacy initiatives
- Ensure compliance with requirements
- Promote privacy culture

13.2 Data Protection Officer (if applicable)

- Inform and advise on privacy obligations
- Monitor compliance with regulations and policies
- Provide advice on data protection impact assessments
- Cooperate with supervisory authorities
- Act as a contact point for supervisory authorities
- Act as a contact point for data subjects
- Report privacy status to management

13.3 Privacy Team

- Develop and maintain privacy policies and procedures
- Provide privacy guidance and expertise
- Conduct privacy impact assessments
- Monitor privacy compliance
- Investigate privacy incidents
- Coordinate privacy training and awareness
- Report privacy status to management

13.4 Department Managers

- Ensure staff compliance with privacy policies
- Identify and address privacy risks in their areas
- Support privacy assessments and audits
- Implement privacy controls in their areas
- Report privacy issues and incidents
- Promote privacy awareness in their teams
- Support privacy improvement initiatives

13.5 All Staff

- Comply with privacy policies and procedures
- Handle personal data according to requirements
- Report privacy incidents and concerns
- Participate in privacy training
- Support privacy assessments and audits
- Suggest privacy improvements

iso27001kit.com

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

- Protect personal data in their activities

14. Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Privacy Officer or equivalent - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

15. Related Documents

- Information Security Policy
- Data Protection Policy
- Records Management Policy
- Incident Response Policy
- Acceptable Use Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

16. Approval

This Privacy Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____

iso27001kit.com

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com