SAMPLE PRIVACY POLICY TEMPLATE

For ISO/IEC 27701:2025 Implementation

Instructions for Use:

- Replace all text in [BRACKETS] with your organization's specific information
- Customize the policy to reflect your actual operations and commitments
- Ensure top management reviews and approves the final policy
- This template meets all four ISO/IEC 27701:2025 content requirements

---

PRIVACY POLICY

Document Control Information

Field	Information
Organization	[Your Organization Name]
Version	[e.g., 1.0]
Effective Date	[DD Month YYYY]
Next Review Date	[DD Month YYYY - typically 12 months from effective date]
Document Owner	[Chief Privacy Officer / Data Protection Officer]
Classification	[Internal / Confidential / Public]
Approved by	[CEO Name and Title]
Approval Date	[DD Month YYYY]

---

1. Purpose and Scope

This Privacy Policy establishes [Organization Name]'s commitment to protecting personal information and provides the framework for our Privacy Information Management System (PIMS).

This policy applies to:

- All [Organization Name] operations [specify: globally / in specific regions]
- All employees, contractors, and temporary staff
- All third parties processing personal data on our behalf
- [Add any other applicable scope elements]

---

2. Our Commitment to Privacy

[REQUIREMENT A: APPROPRIATE TO ORGANIZATION'S PURPOSE]

[Organization Name] is committed to protecting the privacy and personal information of [list your key stakeholders: customers, employees, patients, students, citizens, etc.].

As a [describe your organization type: healthcare provider / financial services company / educational institution / e-commerce platform / government agency / etc.], we process personal information to [describe your primary purposes]:

- [Purpose 1: e.g., "deliver healthcare services to our patients"]
- [Purpose 2: e.g., "fulfill customer orders and provide support"]
- [Purpose 3: e.g., "manage employee relationships"]
- [Purpose 4: e.g., "comply with legal and regulatory obligations"]
- [Add other purposes relevant to your organization]

Privacy is fundamental to [describe why privacy matters to your organization: maintaining trust / fulfilling our mission / meeting legal obligations / competitive advantage / ethical values].

---

3. Our Privacy Principles

We are committed to the following privacy principles:

Transparency We are open and clear about how we collect, use, and protect personal information.

Purpose Limitation We process personal information only for specified, legitimate purposes and do not use it in ways incompatible with those purposes.

Data Minimization We collect and retain only personal information that is necessary for our stated purposes.

Accuracy We take reasonable steps to ensure personal information is accurate, complete, and up-to-date.

Storage Limitation We retain personal information only as long as necessary for the purposes for which it was collected or as required by law.

Security We implement appropriate technical and organizational measures to protect personal information against unauthorized access, loss, destruction, or damage.

Accountability We take responsibility for our personal information processing activities and demonstrate compliance with privacy obligations.

[Add any additional principles specific to your organization or industry]

---

4. Framework for Privacy Objectives

[REQUIREMENT B: FRAMEWORK FOR SETTING PRIVACY OBJECTIVES]

This Privacy Policy provides the foundation for establishing specific, measurable privacy objectives that support our strategic goals.

Our privacy objectives will:

- Align with [Organization Name]'s business strategy and values
- Be specific, measurable, achievable, relevant, and time-bound (SMART)
- Address the needs and expectations of our stakeholders
- Be reviewed and updated regularly

- Be communicated throughout the organization

Current Privacy Objective Focus Areas:

[List your key focus areas for privacy objectives, for example:]

- Response times to data subject requests
- Privacy-by-design implementation in [products/services/systems]
- Employee privacy awareness and training
- Third-party privacy compliance and vendor management
- Privacy incident prevention and response
- [Add other focus areas relevant to your organization]

Specific privacy objectives are documented separately and reviewed [frequency: quarterly / semi-annually / annually].

---

5. Compliance Commitment

[REQUIREMENT C: COMMITMENT TO MEET APPLICABLE REQUIREMENTS]

[Organization Name] is committed to complying with all applicable privacy and data protection laws, regulations, and standards, including:

Legal and Regulatory Requirements: [List applicable laws and regulations for your organization, for example:]

- European Union General Data Protection Regulation (GDPR)
- [Country] Data Protection Act [Year]
- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada
- [Sector-specific regulations: HIPAA, COPPA, GLBA, PCI DSS, etc.]
- [Other national or regional privacy laws applicable to your operations]

Standards and Frameworks:

- ISO/IEC 27701:2025 (Privacy Information Management)
- ISO/IEC 27001:2022 (Information Security Management)
- [Other applicable standards or frameworks]

Contractual and Business Commitments: We honor all privacy commitments in:

- Customer contracts and service level agreements
- Processor and sub-processor agreements
- Partnership agreements
- Industry codes of conduct
- Internal policies and procedures

[If applicable - For Organizations Acting as Processors:]

As a data processor for our clients, we:

- Process personal information only on documented instructions from our controller clients
- Assist our clients in meeting their data protection obligations
- Support our clients in responding to data subject requests
- Notify our clients of personal data breaches without undue delay
- Implement appropriate security measures as agreed with our clients

[If applicable - For Organizations Acting as Controllers:]

As a data controller, we:

- Ensure we have a lawful basis for all personal data processing
- Provide transparent information to data subjects about our processing activities
- Enable data subjects to exercise their privacy rights
- Conduct Data Protection Impact Assessments for high-risk processing
- Maintain records of our processing activities

[Customize this section based on your organization's role and obligations]

---

6. Continual Improvement

[REQUIREMENT D: COMMITMENT TO CONTINUAL IMPROVEMENT]

[Organization Name] is committed to continually improving our Privacy Information Management System.

We will achieve continual improvement through:

Regular Review and Assessment

- Annual review of this Privacy Policy
- [Frequency: Quarterly / Semi-annual / Annual] review of privacy processes and controls
- Regular privacy risk assessments
- Internal privacy audits
- Management review of PIMS performance

Learning and Adaptation

- Learning from privacy incidents, near-misses, and complaints
- Analyzing root causes and implementing preventive measures
- Sharing lessons learned across the organization
- Monitoring privacy incidents affecting our industry

Monitoring Regulatory Developments

- Tracking changes in privacy laws and regulations
- Adopting new regulatory requirements proactively
- Participating in industry privacy forums and working groups
- Engaging with supervisory authorities as appropriate

Adopting Best Practices and Innovation

- Investing in privacy-enhancing technologies
- Implementing privacy-by-design and privacy-by-default approaches
- Benchmarking against industry leaders and best practices
- Researching and piloting innovative privacy solutions

Progressive Standards

- Progressively raising our privacy standards beyond minimum compliance
- Setting increasingly ambitious privacy objectives
- Striving for privacy excellence, not just adequacy

We measure our improvement through:

- [List key performance indicators, for example:]
- Data subject request response times
- Privacy training completion rates
- Privacy incident frequency and severity
- Privacy objective achievement rates
- Customer satisfaction with privacy practices
- Audit findings and closure rates

---

7. Roles, Responsibilities, and Governance

Top Management Accountability

Top management is ultimately accountable for privacy and the effectiveness of this Privacy Information Management System.

Privacy Leadership

[Specify the role assigned to ensure PIMS conformity and reporting]

The [Chief Privacy Officer / Data Protection Officer / Privacy Manager] is assigned responsibility and authority for:

- Ensuring the Privacy Information Management System conforms to ISO/IEC 27701:2025 requirements
- Reporting on PIMS performance to top management
- [Add other key responsibilities]

Data Protection Officer [If applicable under GDPR or other regulations]

[If you have a DPO, describe their role:] The Data Protection Officer is responsible for:

- Monitoring compliance with data protection laws
- Providing advice on data protection obligations
- Advising on Data Protection Impact Assessments
- Cooperating with supervisory authorities
- Acting as contact point for data subjects and supervisory authorities

All Employees

All employees, contractors, and third parties working on behalf of [Organization Name] are responsible for:

- Handling personal information in accordance with this policy and our privacy procedures
- Completing required privacy training
- Reporting privacy concerns, incidents, or potential violations immediately
- Following privacy-by-design principles in their work
- Protecting personal information from unauthorized access, use, or disclosure

Department-Specific Responsibilities

[Customize based on your organization structure:]

- **[CTO / IT Director]:** Technical privacy controls, privacy-by-design, secure development
- **[CMO / Marketing Director]:** Marketing consent compliance, transparent communications
- **[CHRO / HR Director]:** Employee privacy, workplace monitoring transparency
- **[COO / Operations Director]:** Operational privacy controls, business process compliance
- **[CFO / Finance Director]:** Financial data privacy, vendor privacy assessments

Detailed privacy roles and responsibilities are documented in [reference to RACI matrix / roles and responsibilities document / job descriptions].

---

8. Privacy Training and Awareness

All personnel with access to personal information will receive:

- Privacy awareness training during onboarding
- [Frequency: Annual / Bi-annual] privacy refresher training
- Role-specific privacy training as applicable
- Updates on privacy policy and procedure changes

Training completion is tracked and reported to management.

---

9. Privacy Risk Management

We systematically identify, assess, and mitigate privacy risks through:

- Regular privacy risk assessments
- Data Protection Impact Assessments (DPIAs) for high-risk processing
- Privacy impact reviews for new projects, systems, and services
- Ongoing monitoring of privacy controls

- Incident response and breach management procedures

---

10. Privacy by Design and Default

Privacy is embedded into:

- Product and service design from the earliest stages
- System development and procurement
- Business processes and operations
- Organizational practices and culture

We implement privacy-by-default settings that automatically provide the highest level of privacy protection.

---

11. Data Subject Rights

[If applicable under GDPR or similar laws]

We respect and facilitate the exercise of data subject rights, including:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making and profiling

[Customize based on applicable laws]

We respond to valid data subject requests within [specify timeframe: 30 days under GDPR / timeframe under applicable law].

---

12. Third-Party Privacy Management

We ensure that third parties processing personal information on our behalf:

- Are carefully selected based on privacy and security capabilities
- Sign appropriate data processing agreements
- Implement adequate technical and organizational measures
- Process personal information only on our documented instructions
- Are subject to regular privacy compliance assessments

---

13. Privacy Incident Management

We have established procedures to:

- Detect and report privacy incidents promptly
- Investigate and contain privacy incidents
- Assess the risk to affected individuals
- Notify supervisory authorities and affected individuals when required by law
- Document incidents and corrective actions
- Learn from incidents to prevent recurrence

---

14. Policy Review and Updates

This Privacy Policy will be:

- Reviewed at least annually
- Updated when significant changes occur in:

- Our business operations
    - Applicable laws or regulations
    - Technology or security landscape
    - Stakeholder requirements
- Approved by [CEO / Board of Directors] upon recommendation from the [Chief Privacy Officer]

All updates will be communicated to employees and, where appropriate, to other interested parties.

---

15. Questions and Contact Information

Questions, concerns, or requests regarding this Privacy Policy or privacy matters should be directed to:

[Privacy Contact Information]

[Role Title: Chief Privacy Officer / Data Protection Officer]
[Organization Name]
[Email: privacy@organization.com]
[Phone: +XX XXX XXX XXXX]
[Address: if applicable]

For data subject rights requests: [email or web form link]

For privacy complaints: [email or complaint procedure link]

To report a privacy incident: [email or incident reporting link]

---

16. Policy Approval

This Privacy Policy has been reviewed and approved by top management.

Approved by:

[Name]
[Title: Chief Executive Officer / Managing Director]
[Date]

Document Version History

Version	Date	Changes Made	Approved By
1.0	[Date]	Initial policy	[CEO Name]

Distribution and Communication

This Privacy Policy is:

- Communicated to all employees through [methods: intranet posting, onboarding, training, email]
- Available to interested parties upon request to [privacy contact email]
- Reviewed with all new employees during onboarding
- Referenced in employee handbook
- [Add other distribution methods]