## **ISO 27001 Privacy Policy Template**

### **1. Introduction**

This document outlines the Privacy Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes guidelines for safeguarding personal data and respecting individuals’ privacy rights in alignment with applicable data protection laws. For example, compliance with GDPR requires organizations to implement lawful processing and protect data subjects’ rights.

### **2. Purpose**

The purpose of this policy is to:

1. Define processes for collecting, processing, and storing personal data securely.
2. Ensure compliance with data protection regulations, such as GDPR or CCPA.
3. Establish roles and responsibilities for data privacy management.
4. Foster trust by demonstrating the organization’s commitment to protecting personal data.

### **3. Scope**

This policy applies to all employees, contractors, and third-party vendors involved in processing personal data on behalf of [Organization Name]. It encompasses:

* Personal data collected from employees, customers, and other stakeholders.
* Data stored in physical or digital formats.
* Data processing activities, both within and outside organizational systems.

### **4. Policy Statement**

[Organization Name] is committed to ensuring that personal data is collected, processed, and stored in a manner that protects privacy and aligns with ISO 27001 standards. Key principles include:

1. Collecting only the minimum data required for legitimate purposes.
2. Ensuring transparency in data collection and usage.
3. Applying appropriate security measures to protect personal data.

### **5. Data Collection and Processing**

1. Collect personal data only with valid legal grounds, such as explicit consent for marketing, contractual necessity for billing, or compliance with legal obligations.
2. Process personal data solely for specified and legitimate purposes.
3. Maintain accuracy and ensure data is up-to-date.
4. Limit access to personal data based on job roles and responsibilities.

### **6. Data Protection Measures**

1. Encrypt personal data during storage and transmission using strong encryption standards, such as AES-256.
2. Implement role-based access controls to restrict unauthorized access.
3. Regularly review and update security measures to address evolving risks.
4. Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing activities.
5. Implement role-based access controls to restrict unauthorized access.
6. Regularly review and update security measures to address evolving risks.
7. Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing activities.

### **7. Data Subject Rights**

1. Provide individuals with access to their personal data upon request, following a defined process and timeline in accordance with applicable laws.
2. Respond to requests for data correction, deletion, or portability within specified timeframes.
3. Notify individuals of their rights and the process for exercising them, ensuring all necessary information is easily accessible.
4. Respond to requests for data correction, deletion, or portability within specified timeframes.
5. Notify individuals of their rights and the process for exercising them.

### **8. Incident Management**

1. Report data breaches or privacy incidents to the Data Protection Officer immediately.
2. Notify affected individuals and regulatory authorities as required by law.
3. Document all incidents and corrective actions taken.

### **9. Compliance and Monitoring**

1. Conduct regular audits to ensure compliance with this policy and applicable regulations.
2. Address non-compliance with corrective actions or disciplinary measures.
3. Provide regular reports on privacy compliance to executive leadership.

### **10. Related Documentation**

1. Information Security Policy
2. Data Retention Policy
3. Incident Management Policy

### **11. Review and Revision**

This policy will be reviewed annually or when significant changes occur in data protection laws or organizational practices. Updates will be approved by the Data Protection Officer and executive leadership.

### **Appendix A: Data Inventory Template**

| **Data Type** | **Source** | **Purpose** | **Retention Period** | **Protection Measures** |
| --- | --- | --- | --- | --- |
| ----------------- | ------------------ | ------------------ | ------------------ | --------------------------- |
|  |  |  |  |  |

### **Appendix B: Privacy Incident Report Template**

| Incident ID | Date/Time | Affected Data Type | Description of Incident | Actions Taken | Resolution Status |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

### **Appendix C: Policy Acknowledgment Form**

I acknowledge that I have read and understood the Privacy Policy and agree to comply with its requirements.

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_