

Privacy and Data Protection Policy

Purpose

Your Organization handles personal information about customers, users, employees, and other individuals. This policy sets how that information is collected, used, shared, kept, and protected, so that Your Organization treats people fairly and meets the privacy laws and contract terms that apply to it.

This policy is a framework for the privacy program. It is not legal advice. Counsel should confirm which laws apply to Your Organization (for example, the GDPR, UK GDPR, CCPA/CPRA and other U.S. state laws, HIPAA, or sector rules) and adapt the requirements below.

Scope

This policy applies to all workforce members and to all processing of personal information by or for Your Organization, in any form and system, including processing carried out by vendors on Your Organization's behalf. "Personal information" means any information relating to an identified or identifiable individual.

Roles and responsibilities

- **The privacy lead (or Data Protection Officer, where one is required)** owns this policy, advises on privacy questions, runs impact assessments, and handles regulator and individual contact.
- **Data owners** are accountable for the personal information in their business area, including purpose, retention, and sharing.
- **The security team** implements the technical and organizational safeguards.
- **All workforce members** collect and use personal information only as their role requires and report suspected incidents immediately.

Principles

Your Organization processes personal information according to these principles:

1. **Lawful, fair, and transparent.** There is a documented lawful basis or permitted purpose, and people are told what happens to their information.
2. **Purpose limitation.** Information is collected for specified purposes and not used for incompatible new purposes without a new assessment and, where required, notice or consent.
3. **Data minimization.** Only the information needed for the purpose is collected and kept.
4. **Accuracy.** Information is kept accurate and corrected when errors are found.
5. **Storage limitation.** Information is kept only as long as needed, following the Data Retention Policy.
6. **Integrity and confidentiality.** Information is protected by the safeguards in the Information Security Policy and its supporting policies.
7. **Accountability.** Your Organization can show how it meets these principles.

Requirements

1. Records of processing

The privacy lead maintains a record of processing activities listing each activity, its purpose, the categories of individuals and data, the recipients, the transfers outside the original jurisdiction, the retention period, and the safeguards. Data owners update it when processing changes.

2. Notice and lawful basis

- Public-facing privacy notices describe what is collected, why, the lawful basis or business purpose, who receives it, how long it is kept, and how to exercise rights.
- Consent, where used, is specific, informed, recorded, and as easy to withdraw as it was to give.
- Special or sensitive categories of data (for example, health, biometric, precise location, children's data) are processed only with an approved basis and added safeguards.

Counsel to confirm: which lawful bases or permitted purposes apply, when consent is required and what form it must take, and which categories of data count as special or sensitive. These differ between laws such as the GDPR and U.S. state privacy laws.

3. Individual rights

Your Organization honors the rights that apply to the individual, which may include access, correction, deletion, restriction, portability, objection, and opt-out of sale or sharing. Requests are logged, identity is verified, and responses are sent within the deadline the applicable law sets. Staff who receive a request forward it to the privacy lead the same day.

Counsel to confirm: which rights apply to which individuals, and the response deadline and any permitted extension for each law that applies (for example, one month under the GDPR and 45 days under the CCPA, each extendable in some circumstances).

4. Privacy by design and impact assessments

- New products, features, vendors, and data uses that involve personal information are assessed for privacy risk before launch.
- A data protection impact assessment is completed where processing is likely to result in high risk, such as large-scale sensitive data, systematic monitoring, profiling with significant effect, or new technologies. The assessment records the risks and the measures adopted.
- Default settings are the most privacy-protective that still allow the service to work.

5. Vendors and processors

- Vendors that process personal information on Your Organization's behalf are assessed under the Vendor Risk Management Policy and are bound by a written data processing agreement covering instructions, confidentiality, security, subprocessors, assistance with rights requests, breach notice, return or deletion, and audit.
- A current list of subprocessors is maintained and made available where required.

6. International transfers

Personal information is transferred across borders only under a recognized transfer mechanism or exemption, documented by the privacy lead, and after a transfer risk assessment where required.

Counsel to confirm: whether any transfer restrictions apply to Your Organization, and which mechanisms and assessments are recognized for each route.

7. Security of personal information

Personal information is protected with access control, encryption in transit and at rest, logging, backup, and the other controls in the information security policy set. Access is limited to people who need it for their role.

8. Incidents and breaches

Suspected loss, theft, or unauthorized access or disclosure of personal information is reported immediately under the Incident Response Plan. The privacy lead decides, with legal counsel, whether notice to regulators and affected individuals is required and ensures it is sent within the legal deadline (for example, 72 hours to a supervisory authority under the GDPR where it applies).

Counsel to confirm: the notification triggers, recipients, deadlines and content for each law and contract that applies, including U.S. state breach-notification laws, which vary by state.

9. Retention and disposal

Personal information is deleted or de-identified when its retention period ends, following the Data Retention Policy and Media Protection Policy, subject to legal holds.

10. Training and awareness

All workforce members complete privacy training on hire and annually. People who handle rights requests or sensitive data receive role-specific training.

Exceptions

Exceptions require written approval from the privacy lead and the security team, with the risk stated and a review date.

Enforcement

Misuse of personal information may result in disciplinary action up to and including termination, and may carry legal consequences for the individual and for Your Organization.

Evidence

Evidence of operation includes the record of processing, privacy notices, rights-request log, impact assessments, data processing agreements, training records, and incident records.

Review cadence

This policy is reviewed annually by the privacy lead and legal counsel, or sooner when laws, products, or data uses change materially.

Effective date: [the date this policy takes effect]