

Privacy Program Manual

Use these records to document privacy governance and the actual handling of personal data. Complete applicability, legal bases and deadlines with the responsible privacy or legal function; keep controller and processor responsibilities distinct where they differ.

Complete bracketed fields with approved information. Duplicate modules and rows as needed; record the reason for any section marked not applicable.

Document [ID and revision] **Owner** [Role] **Scope** [Organization, site or product]

Effective date [Date] **Approval** [Controlled record] **Next review** [Date or trigger]

Program foundations

Foundation	Approved program position
Purpose scope and entities	[Activities, locations, data and role in processing]
Applicable obligations	[Regime, requirement, applicability assessment and reviewer]
Privacy principles and commitments	[Adopted policy text and source]
Boundaries and related programs	[Security, records and incident interfaces]

Governance and accountability

Role or body	Duties and authority	Reporting and independence
[Privacy office or designated role]	[Advice, oversight and decisions]	[Reporting line and safeguards]
[Process or data owner]	[Operational accountability]	[Escalation and review]
[Committee or external party]	[Approved responsibility]	[Handoff and agreement]

Data inventory and records of processing

Repeat the record for each processing activity and identify how it stays current.

Activity record	Complete with verified data
Activity purpose and role	[Activity ID; controller / processor; purpose]
People and data categories	[Subjects, categories, sources and sensitive data]
Basis recipients and transfers	[Reviewed basis, recipients and transfer locations]
Retention and safeguards	[Approved rule, deletion trigger and protection]
Inventory maintenance	[Owner, change trigger, last review and evidence]

Privacy risk and impact assessments

Assessment field	Decision and evidence
Screening and scope	[Activity, change, screening criteria and decision to assess]
Data flow and necessity	[Purpose, collection, access, use, disclosure and alternatives]
Risk and mitigation	[Impact on individuals, criteria, control and residual risk]
Consultation and approval	[Consulted roles, unresolved issues and authorized decision]

Transparency and individual rights

Notice or consent record	Approved wording and operation
Notice and audience	[Version, channel, language and delivery trigger]
Consent or preference	[Where applicable: choice, evidence, withdrawal and downstream effect]

Rights request case form

Request stage	Complete for this request
Intake and scope	[Case ID, request type, receipt time and relevant activity]
Identity and authority check	[Proportionate check and evidence; access restriction]
Deadline and clock	[Applicable reviewed rule, start, permitted extension and due date]
Search and assessment	[Systems, data found, restrictions and decision authority]
Response and completion	[Approved response, secure channel, delivery and retained record]

Third parties and data transfers

Vendor or transfer	Assessment and safeguards	Decision and review
[Processing, role, location and recipients]	[Due diligence, contract, mechanism and supporting review]	[Authority, conditions and change trigger]

Data security and records management

Data or record group	Handling and access	Retention and disposal
[Activity and data category]	[Approved safeguards and role access]	[Rule, trigger, method and evidence]
[Restricted record]	[Transfer and disclosure controls]	[Hold conditions and authorized disposal]

Secure disposal work record

1. Identify [data and locations], [retention trigger] and any [hold or restriction].
2. Obtain [required authorization] and perform the approved [disposal method].
3. Verify [affected copies and downstream recipients] as required by the adopted process.
4. Record [completion evidence], [exceptions] and [reviewer].

Privacy incident and breach response

Response stage	Decision record	
Discovery and protection	[Time, source, affected processing and authorized immediate action]	
Triage and investigation	[Data, individuals, scope, facts and evidence access]	
Notification assessment	[Applicable rule, clock start, recipients, decision and rationale]	
Response and remediation	[Approved notices, containment, recovery and corrective actions]	
Closure and review	[Decision authority, evidence, retention and lessons]	
Response role	Decision rights	Coordination and contact reference
[Privacy, legal, security or business role]	[Assessment or notification authority]	[Verified directory and handoff]

Training and awareness

Audience and activity	Learning objective and material	Evidence and follow up
[Role handling personal data]	[Policy, procedure and adopted frequency]	[Attendance, understanding check and gaps]

Privacy learning exercise

Exercise element	Complete from your approved process
Situation and question	[Scenario based on the organization's actual processing]
Expected response	[Decision, escalation and governing rule]
Understanding check	[Question, approved answer and feedback]

Monitoring audit and improvement

Review area	Measure or evidence	Finding and action
[Inventory, rights, vendors or incidents]	[Definition, source, frequency and criterion]	[Result, owner and due date]
[Management review]	[Inputs and unresolved risks]	[Decision and effectiveness follow-up]

Glossary

Term	Program definition	Source and regime
[Personal data or adopted term]	[Approved definition]	[Controlled source]
[Controller processor or other role]	[Meaning for this program]	[Applicable source]

Release review

- ☐ Activity records, legal applicability, deadlines and notification decisions have been reviewed.
- ☐ Notices, vendor safeguards, retention and operational procedures agree with actual processing.

Reviewer role	Decision and date	Open actions and approval reference
[Role]	[Approved or returned]	[Record and next review]