ORGANIZATION FOR DIGITAL INFORMATION PRIVACY & AWARENESS

Corporate Privacy Certification Criteria

Version 1.0 Draft · Effective date, Pending counsel review

Status. Draft for public comment and counsel review. Not yet in force for any assessment.

What certification attests

ODIPA certification is a conformity assessment. It attests that, on the assessment date, an organization met the criteria in this document as evidenced to ODIPA-qualified assessors. The criteria draw on established privacy and security frameworks, and each criterion cites the provisions that informed it.

Certification is not a determination of legal compliance. Only regulators and courts can make that determination. Framework references show where a criterion comes from. They do not certify that an organization complies with the cited law.

Rating scale

Met	Evidence demonstrates the requirement is implemented and operating.
Partially Met	The requirement is implemented in part or operates inconsistently. A finding is issued with a remediation window.
Not Met	Evidence is absent or the practice contradicts the requirement. A finding is issued and certification cannot issue until remediated.
Not Applicable	The requirement does not apply to the organization's processing, with the rationale documented by the assessor.

Certification decision rule

1. Every criterion marked Mandatory must be rated Met or Not Applicable for certification to issue.

2. Criteria not marked Mandatory may be rated Partially Met, provided the organization accepts a remediation plan with a dated window, and no more than one quarter of applicable non-mandatory criteria are rated below Met.

3. All findings are delivered in writing with the criterion cited by identifier. The organization remediates and resubmits evidence. Certification issues only when the decision rule is satisfied on the assessment date.

4. Certification attests conformance to these criteria on the assessment date. It is not a determination of legal compliance, which only regulators and courts can make.

42 criteria across 7 domains, 26 mandatory.

GOV · Governance and Accountability

Whether privacy is owned, documented, and overseen as a program rather than treated as a policy page.

GOV-01 · Designated privacy owner MANDATORY

A named individual or role is accountable for the privacy program, with documented responsibilities and executive reporting.

Evidence accepted. Role description or charter; Organization chart

Framework references. GDPR Art. 37 to 39; NIST PF GV.PO; SOC 2 CC1

GOV-02 · Written privacy program MANDATORY

An internal privacy policy or program document defines principles, roles, and procedures, is approved by leadership, and is reviewed at least annually.

Evidence accepted. Internal privacy policy with approval and review dates

Framework references. NIST PF GV.PO; ISO 27001 A.5; SOC 2 CC1

GOV-03 · Data inventory MANDATORY

The organization maintains a current inventory of personal information it processes, including categories, sources, purposes, recipients, and retention, updated when processing changes.

Evidence accepted. Data inventory or record of processing activities

Framework references. GDPR Art. 30; CCPA §1798.100; NIST PF ID.IM

GOV-04 · Privacy risk assessment

New or materially changed processing of personal information is assessed for privacy risk before launch, with documented outcomes and mitigations.

Evidence accepted. PIA or DPIA template; Completed assessment samples

Framework references. GDPR Art. 35; NIST PF ID.RA; SOC 2 CC3

GOV-05 · Retention schedule MANDATORY

A retention and deletion schedule defines how long each category of personal information is kept and the basis for that period.

Evidence accepted. Retention and deletion schedule

Framework references. GDPR Art. 5(1)(e); CCPA §1798.100(a)(3); SOC 2 P4

GOV-06 · Data classification

Personal information is classified by sensitivity, and handling requirements are defined for each class.

Evidence accepted. Data classification policy

Framework references. ISO 27001 A.5; NIST PF ID.IM

GOV-07 · Leadership oversight

Privacy program status, incidents, and risks are reported to executive leadership or the board at least annually.

Evidence accepted. Meeting minutes or reporting decks, redacted

Framework references. NIST PF GV.MT; SOC 2 CC1

TRN · Transparency and Consent

Whether people are told the truth about processing, at the right time, and given real choices.

TRN-01 · Complete privacy notice MANDATORY

A consumer-facing privacy notice accurately describes categories collected, sources, purposes, disclosures, retention, consumer rights, and contact methods, and carries an effective date.

Evidence accepted. Current privacy notice; Change history

Framework references. CCPA §1798.130; GDPR Art. 13 and 14; SOC 2 P1

TRN-02 · Notice at collection MANDATORY

Consumers are informed at or before the point of collection of the categories collected and the purposes of use.

Evidence accepted. Collection point screenshots; Notice placement documentation

Framework references. CCPA §1798.100(b); GDPR Art. 13

TRN-03 · Consent where required MANDATORY

Where law or the organization's own notice requires consent, it is obtained through an affirmative act, is specific to the purpose, and is recorded.

Evidence accepted. Consent flow documentation; Consent records sample

Framework references. GDPR Art. 6 and 7; CCPA sensitive information rules; SOC 2 P2

TRN-04 · Opt-out of sale and sharing MANDATORY

Where applicable, consumers can opt out of the sale or sharing of personal information through an accessible mechanism, and browser opt-out preference signals are honored.

Evidence accepted. Opt-out mechanism; Preference signal handling documentation

Framework references. CCPA §1798.120 and §1798.135; CPRA regulations

TRN-05 · No manipulative design

Consent, opt-out, and rights interfaces are designed so that declining is as easy as accepting and choices are not obtained through confusing or coercive design.

Evidence accepted. Interface review; Design guidelines

Framework references. CPRA regulations on dark patterns; GDPR Art. 7(3)

TRN-06 · Children's data

Where the organization knowingly processes children's personal information, age screening, parental consent, and heightened protections are implemented as applicable.

Evidence accepted. Age screening and consent procedures

Framework references. COPPA, 16 CFR Part 312; CCPA §1798.120(c); GDPR Art. 8

RTS · Individual Rights

Whether people can actually exercise their rights, on time, without being punished for it.

RTS-01 · Request channels MANDATORY

Consumers can submit rights requests through at least the methods required by applicable law, and the channels are published in the privacy notice.

Evidence accepted. Request intake documentation

Framework references. CCPA §1798.130(a); GDPR Art. 12

RTS-02 · Proportionate verification MANDATORY

Requester identity is verified using methods proportionate to the sensitivity of the data and the request, without collecting unnecessary additional information.

Evidence accepted. Verification procedure

Framework references. CPRA regulations on verification; GDPR Art. 12(6)

RTS-03 · Timeliness MANDATORY

Requests are tracked and fulfilled within statutory timelines, with extensions used only where permitted and communicated.

Evidence accepted. Request log with dates; Timeline tracking

Framework references. CCPA §1798.130(a)(2); GDPR Art. 12(3)

RTS-04 · Access and portability MANDATORY

Access requests return the specific personal information held, in a usable and where required portable format.

Evidence accepted. Fulfilled request samples, anonymized

Framework references. CCPA §1798.110; GDPR Art. 15 and 20; SOC 2 P5

RTS-05 · Deletion including processors MANDATORY

Deletion requests are fulfilled across the organization's systems and communicated to service providers and third parties as required.

Evidence accepted. Deletion procedure; Processor notification records

Framework references. CCPA §1798.105; GDPR Art. 17 and 19

RTS-06 · Correction

Consumers can correct inaccurate personal information, and corrections propagate to relevant systems and recipients.

Evidence accepted. Correction procedure

Framework references. CCPA §1798.106; GDPR Art. 16

RTS-07 · Denials, appeals, and non-discrimination MANDATORY

Denied requests are documented with reasons and any appeal route, and consumers are not discriminated against for exercising rights.

Evidence accepted. Denial records; Non-discrimination policy

Framework references. CCPA §1798.125; GDPR Art. 12(4); CPA and VCDPA appeal provisions

MIN · Data Minimization and Retention

Whether the organization collects only what it needs and lets go of it when it should.

MIN-01 · Purpose limitation MANDATORY

Personal information is used only for the purposes disclosed at collection or purposes compatible with them.

Evidence accepted. Purpose documentation in the inventory; Use case review records

Framework references. GDPR Art. 5(1)(b); CCPA §1798.100(c); SOC 2 P3

MIN-02 · Collection limitation MANDATORY

Collection is limited to what is reasonably necessary and proportionate for the disclosed purposes.

Evidence accepted. Data element justification; Form and collection point review

Framework references. GDPR Art. 5(1)(c); CCPA §1798.100(c); NIST PF CT.DM

MIN-03 · Retention enforced

Retention periods are enforced through technical or procedural controls, not only stated in policy.

Evidence accepted. Deletion job evidence; Retention control documentation

Framework references. GDPR Art. 5(1)(e); SOC 2 P4

MIN-04 · Secure disposal

Personal information beyond its retention period is disposed of securely, including on backups within a defined period and at vendors.

Evidence accepted. Disposal procedure; Media sanitization standard

Framework references. ISO 27001 A.7 and A.8; SOC 2 P4

MIN-05 · De-identification standard

Where the organization relies on de-identified or aggregated data, the method meets a recognized standard and re-identification is contractually and technically prohibited.

Evidence accepted. De-identification methodology; Contract terms

Framework references. CCPA §1798.140 de-identified definition; GDPR Recital 26

SEC · Security Safeguards

Whether the information is protected in proportion to its sensitivity, and whether the organization would know if it were not.

SEC-01 · Information security program MANDATORY

A written information security program defines controls proportionate to the sensitivity and volume of personal information processed.

Evidence accepted. Information security policy

Framework references. CCPA §1798.150 and Civil Code §1798.81.5; GDPR Art. 32; ISO 27001 A.5

SEC-02 · Access control MANDATORY

Access to personal information follows least privilege, is reviewed periodically, and administrative and remote access require multi-factor authentication.

Evidence accepted. Access control policy; Access review records

Framework references. ISO 27001 A.5 and A.8; SOC 2 CC6; NIST PF PR.AC

SEC-03 · Encryption MANDATORY

Personal information is encrypted in transit and, for sensitive categories, at rest, using current standards with managed keys.

Evidence accepted. Encryption standard; Key management documentation

Framework references. GDPR Art. 32; ISO 27001 A.8; SOC 2 CC6

SEC-04 · Logging and monitoring

Access to and changes in systems holding personal information are logged, retained, and monitored for anomalies.

Evidence accepted. Logging standard; Monitoring evidence

Framework references. ISO 27001 A.8; SOC 2 CC7

SEC-05 · Vulnerability management MANDATORY

Systems are assessed for vulnerabilities on a defined cadence, including at least annual independent testing for internet-facing systems, and findings are remediated by severity.

Evidence accepted. Most recent test summary; Remediation tracking

Framework references. ISO 27001 A.8; SOC 2 CC7

SEC-06 · Secure development

Systems that process personal information are built and changed under a process that includes security and privacy review before release.

Evidence accepted. SDLC documentation; Change management records

Framework references. GDPR Art. 25; ISO 27001 A.8; NIST PF PR.PO

SEC-07 · Incident response MANDATORY

An incident response plan assigns roles, defines escalation, and is exercised at least annually.

Evidence accepted. Incident response plan; Exercise records

Framework references. ISO 27001 A.5; SOC 2 CC7; NIST PF PR.PO

SEC-08 · Breach notification MANDATORY

A breach procedure determines notification obligations and executes notice to individuals, regulators, and partners within statutory timeframes.

Evidence accepted. Breach notification procedure; Decision log template

Framework references. GDPR Art. 33 and 34; Civil Code §1798.82; HIPAA Breach Notification Rule where applicable

VEN · Vendors and Third Parties

Whether the organization's promises survive the handoff to everyone it shares data with.

VEN-01 · Processor inventory MANDATORY

Service providers and third parties that receive personal information are inventoried with the data shared and the purpose.

Evidence accepted. Vendor and sub-processor list

Framework references. GDPR Art. 28 and 30; CCPA §1798.140 service provider definition

VEN-02 · Due diligence

Vendors are assessed for privacy and security practices before receiving personal information, proportionate to the risk of the sharing.

Evidence accepted. Due diligence questionnaire; Completed assessments

Framework references. SOC 2 CC9; NIST PF ID.DE

VEN-03 · Contract terms MANDATORY

Contracts with recipients of personal information include the terms required by applicable law, including purpose limitation, confidentiality, security, deletion, and cooperation with rights requests.

Evidence accepted. DPA template; Executed agreement samples

Framework references. GDPR Art. 28(3); CCPA §1798.100(d) and §1798.140; SOC 2 P6

VEN-04 · Cross-border transfers

Where personal information leaves its jurisdiction of collection, a lawful transfer mechanism is in place and documented.

Evidence accepted. Transfer mechanism records

Framework references. GDPR Art. 44 to 46; PIPEDA and LGPD transfer provisions where applicable

VEN-05 · Ongoing oversight and offboarding

Vendor performance is monitored, and at termination personal information is returned or destroyed with confirmation.

Evidence accepted. Monitoring records; Offboarding checklist

Framework references. GDPR Art. 28(3)(g); SOC 2 CC9

TRA · Training and Awareness

Whether the people who touch the data know what they are responsible for.

TRA-01 · Onboarding training MANDATORY

New personnel who handle personal information complete privacy training before receiving access.

Evidence accepted. Onboarding procedure; Completion records

Framework references. GDPR Art. 39(1)(b); ISO 27001 A.6; SOC 2 CC1

TRA-02 · Annual role-based training MANDATORY

Personnel complete privacy training at least annually, with content tailored to the data and processes their role involves.

Evidence accepted. Training curriculum; Completion records by role, anonymized

Framework references. CCPA §1798.130(a)(6); ISO 27001 A.6; NIST PF GV.AT

TRA-03 · Handler procedures

Documented procedures exist for personnel who process rights requests, respond to incidents, or handle sensitive categories.

Evidence accepted. Role-specific procedures

Framework references. CCPA §1798.130(a)(6); SOC 2 CC2

TRA-04 · Awareness of reporting

Personnel know how to report suspected incidents and privacy concerns, and reports are acted on without retaliation.

Evidence accepted. Reporting channel documentation; Awareness materials

Framework references. ISO 27001 A.6; SOC 2 CC2 and CC7

This document is generated from the same source as the criteria page at odipa.org/programs/corporate-certification/criteria. The web page is authoritative. Draft pending counsel review. Not yet in force for any assessment.