ODIPA

CORPORATE PRIVACY CERTIFICATION GUIDE

Organization for Digital Information Privacy & Awareness

501(c)(3) Independent Nonprofit Certification Program

Everything your organization needs to understand ODIPA's independent privacy certification process — frameworks covered, assessment methodology, Trust Seal usage, pricing, and how to apply.

TABLE OF CONTENTS

1. ABOUT ODIPA & THIS CERTIFICATION PROGRAM

Who We Are

ODIPA — the Organization for Digital Information Privacy & Awareness — is a California 501(c)(3) nonprofit organization dedicated to consumer privacy education, advocacy, independent research, and open-source technology development. We are not a law firm, a regulatory agency, or a technology vendor. We are an independent nonprofit whose mission is to protect consumer privacy rights in an increasingly data-driven world.

ODIPA's Corporate Privacy Certification program is one of eight integrated programs operated by the organization. Revenue from certification fees directly funds free consumer privacy education, advocacy, and open-source tool development — which is why our certification is not just a credential for your organization but a contribution to the broader privacy ecosystem.

What Makes ODIPA Certification Different

What It Covers	Typical Industry	ODIPA
Self-certification / checklists	No	Yes — independently verified
Legal compliance guarantee	No	No (see Section 10)
Multi-framework coverage	Varies	Yes — 20+ frameworks
Third-party assessors	Varies	Yes — credentialed, independent
Two-assessor panel requirement	Rare	Yes — always
Public Trust Seal	Varies	Yes — consumer-facing
Annual renewal	Varies	Yes — keeps certification current
Conflict of interest policy	Varies	Yes — signed by every assessor
Nonprofit independence	No	Yes — no vendor or investor relationships

2. WHAT CERTIFICATION COVERS

Scope of the Assessment

ODIPA's certification assesses your organization's data practices across five core domains. The specific frameworks applied depend on your industry, size, geography, and the types of data you collect and process. You will work with your assessment team to define the exact scope before the assessment begins.

01

Data Governance & Policies

Privacy policy accuracy, internal data governance documentation, data inventory and classification, retention and deletion policies, and records of processing activities (ROPA).

02

Consumer Rights & Request Handling

Procedures for handling consumer rights requests: access, deletion, correction, portability, opt-out, and the right to know. Response time compliance, request verification procedures, and denial documentation.

03

Data Security & Breach Response

Technical and organizational security measures, encryption standards, access controls, vendor management, breach detection and notification procedures, and incident response plan review.

04

Staff Training & Awareness

Privacy training program documentation, training frequency and content, role-specific training for data handlers, and awareness of applicable regulatory requirements.

05

Third-Party & Vendor Management

Data processing agreements (DPAs), vendor due diligence processes, sub-processor management, cross-border transfer mechanisms, and contractual privacy obligations with partners and service providers.

What Is NOT In Scope

ODIPA does not assess your organization's commercial practices, product quality, financial performance, or employee practices unrelated to data privacy. Certification is scoped to data privacy governance and operations only. Specific systems, products, or subsidiaries may be excluded from scope by agreement before assessment begins.

3. PRIVACY FRAMEWORKS & APPLICABLE LAW

Frameworks We Assess Against

ODIPA assesses against the frameworks and laws applicable to your specific organization based on your industry, size, geography, and data types. The following frameworks are covered by ODIPA-certified assessors. Your engagement will be scoped to the relevant subset before assessment begins.

Category	Frameworks & Laws Covered
U.S. State Privacy Laws	CCPA/CPRA (California), VCDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), MCDPA (Montana), TIPA (Texas), FDBR (Florida), OCPA (Oregon), NHPA (New Hampshire), and additional state laws as enacted
Financial Services	GLBA (Gramm-Leach-Bliley Act), FCRA, BSA/AML data requirements, PCI DSS (payment card), SOX data governance provisions, NYDFS Part 500 (cybersecurity)
Healthcare	HIPAA Privacy Rule, HIPAA Security Rule, HITECH Act, 42 CFR Part 2 (substance use records), FDA 21 CFR Part 11 (electronic records)
Education	FERPA (student records), COPPA (children under 13), CIPA (school internet safety)
Energy & Critical Infrastructure	NERC CIP (critical infrastructure protection), DOE cybersecurity guidelines
Biometric & Sensitive Data	BIPA (Illinois Biometric Information Privacy Act), WA MHMD (My Health MY Data), TX CUBI
International	GDPR (European Union), UK GDPR, LGPD (Brazil), PIPEDA/Law 25 (Canada), PIPL (China), PDPA (Thailand/Singapore variants)
Security Frameworks	NIST Privacy Framework, NIST Cybersecurity Framework, ISO 27001, ISO 27701, SOC 2 Type II
Sector-Specific	COPPA, CAN-SPAM, TCPA (communications), FTC Act Section 5 (unfair/deceptive practices)

Framework coverage is updated as new laws take effect. Your assessment team will confirm the applicable frameworks for your engagement before assessment begins. ODIPA's assessor panel includes specialists across all listed frameworks.

4. THE ASSESSMENT PROCESS — STEP BY STEP

How the Assessment Works

ODIPA's assessment follows a structured six-phase process designed to be thorough, fair, and minimally disruptive to your operations. The typical end-to-end timeline from application to report delivery is 4–8 weeks depending on organization size and assessment complexity.

Phase 1
1–3 days

Application & Scoping

You submit your application and initial organizational profile. Your assigned assessment team reviews your industry, size, data types, and applicable frameworks. A scoping call is scheduled to confirm assessment boundaries, deliverables, timeline, and pricing. You receive a formal Statement of Work for legal review and signature.

Phase 2
5–10 days

Document Request

Your assessment team provides a structured document request list covering: privacy policy and notices, internal data governance documentation, records of processing activities, vendor/DPA agreements, staff training records, breach response procedures, and security policy documentation. You submit materials via ODIPA's secure document portal.

Phase 3
7–14 days

Documentation Review

Lead assessor conducts a structured review of all submitted documentation against applicable frameworks. Initial gap analysis is developed. Clarification questions are submitted in writing. A second assessor independently reviews high-risk findings before proceeding to interviews.

Phase 4
1–2 days

Structured Interview

A 2–3 hour structured interview with your privacy officer, legal counsel, IT security lead, and any additional relevant personnel. The interview covers: how documented policies are implemented in practice, how consumer rights requests are handled, staff training and awareness, and breach response capability. Both assessors participate.

Phase 5
3–5 days

Panel Deliberation & Decision

Both assessors independently draft findings. The two-assessor panel convenes to reconcile findings and reach a consensus certification decision. No individual assessor has unilateral authority to certify or deny. Findings are reviewed for consistency with prior certifications in the same industry.

Phase 6
2–3 days

Report Delivery

You receive a confidential Assessment Report covering: certification decision, findings by domain, gap analysis with prioritized remediation recommendations, framework-specific observations, and (if certified) Trust Seal license and activation instructions. Reports are delivered via secure portal.

5. WHAT ASSESSORS REVIEW

Document Request Checklist

The following represents a typical document request for a mid-market technology or financial services company. Your actual request will be scoped to your specific frameworks and organization type. Not all items are required for every assessment.

Privacy Governance

- ✓ Privacy policy (consumer-facing) — current version with effective date
- ✓ Internal privacy governance policy or privacy program documentation
- ✓ Data inventory or records of processing activities (ROPA)
- ✓ Data classification policy
- ✓ Data retention and deletion schedule
- ✓ Privacy impact assessment (PIA) or data protection impact assessment (DPIA) templates

Consumer Rights

- ✓ Consumer rights request intake procedure
- ✓ Sample completed rights request workflows (anonymized)
- ✓ Request verification and authentication procedures
- ✓ Denial documentation procedure and sample denial records
- ✓ Do Not Sell / Share opt-out mechanism documentation

Security & Breach Response

- ✓ Information security policy
- ✓ Encryption standards documentation
- ✓ Access control and privileged access management policy
- ✓ Breach detection and notification procedure
- ✓ Incident response plan
- ✓ Most recent penetration test or vulnerability assessment summary

Staff Training

- ✓ Privacy training curriculum or program description
- ✓ Training completion records for past 12 months (anonymized by role)
- ✓ Role-specific training documentation for data handlers
- ✓ New employee onboarding privacy training procedure

Vendor Management

- ✓ Data processing agreement (DPA) template
- ✓ Vendor privacy due diligence questionnaire
- ✓ List of key data processors / sub-processors
- ✓ Cross-border transfer mechanisms (SCCs, adequacy decisions, BCRs)
- ✓ Vendor contract privacy addendum procedure

Document Submission

All documents are submitted through ODIPA's secure encrypted document portal. You control what is submitted and may redact employee names, personal data, and commercially sensitive details not relevant to the assessment. ODIPA assessors sign confidentiality agreements before accessing any submitted materials. Documents are retained for 3 years and then securely destroyed.

6. ASSESSOR CREDENTIALS & INDEPENDENCE

Who Conducts Your Assessment

ODIPA's certification assessments are conducted exclusively by volunteer professionals holding active, recognized credentials in privacy law, information security, or compliance. All assessors sign ODIPA's Conflict of Interest Policy before each engagement and are matched to your assessment based on industry expertise and framework specialization.

Credential	Full Name	Issuer	Framework Expertise
CIPP/US	Certified Information Privacy Professional / United States	IAPP	U.S. state and federal privacy law
CIPP/E	Certified Information Privacy Professional / Europe	IAPP	GDPR and EU/UK data protection
CIPM	Certified Information Privacy Manager	IAPP	Privacy program management
CIPT	Certified Information Privacy Technologist	IAPP	Privacy in technology design
CISA	Certified Information Systems Auditor	ISACA	Information systems audit & control
CISSP	Certified Information Systems Security Professional	ISC2	Information security governance
QSA	Qualified Security Assessor	PCI SSC	PCI DSS payment card security
CHPC	Certified HIPAA Privacy & Security Expert	CHPSE	Healthcare privacy & security
CAMS	Certified Anti-Money Laundering Specialist	ACAMS	BSA/AML financial data compliance

Independence Safeguards

Two-Assessor Panel

Every certification decision requires agreement by a minimum two-assessor independent panel. No individual assessor has unilateral authority to certify or deny.

Conflict of Interest Policy

Assessors may not evaluate any organization with which they have a current or recent financial, employment, consulting, or advisory relationship. Signed disclosure required before each engagement.

Assessor–Applicant Separation

Assessors are assigned by ODIPA staff, not selected by applicants. Applicants may request reassignment for documented cause; they may not select their assessors.

Continuing Education Requirement

Assessors must maintain active, current credentials. Lapsed credentials result in immediate suspension from the assessor panel pending renewal.

Confidentiality Commitment

All assessors sign a confidentiality agreement covering all materials submitted during the assessment. Assessment findings are never shared with third parties.

No Commercial Relationships

ODIPA assessors do not sell consulting, remediation, or legal services to organizations they assess. Any assessor who develops a commercial relationship with an applicant is disqualified from that engagement.

7. CERTIFICATION OUTCOMES & THE TRUST SEAL

Possible Outcomes

Certified	Your organization meets all required standards for the assessed frameworks. You receive the ODIPA Trust Seal, a confidential Assessment Report with findings, and a Trust Seal License Agreement. Certification is valid for one year from the date of issuance.
Provisionally Certified	Your organization meets most requirements but has identified gaps in non-critical areas. You receive conditional certification with a remediation plan and a 90-day window to address gaps. Upon remediation verification, full certification is granted.
Not Certified	Your organization has material gaps in one or more assessed domains. You receive a detailed gap analysis report with prioritized remediation recommendations. Re-assessment may be requested after 90 days at a reduced re-assessment fee.

The ODIPA Trust Seal

Certified organizations receive a digital Trust Seal for use on their website, privacy policy, and consumer-facing marketing materials. The Trust Seal is a verifiable signal that your organization has passed an independent third-party privacy assessment — not a self-declared certification.

Permitted Uses

- ✓ Display on your public-facing website on privacy policy or data governance pages
- ✓ Inclusion in your privacy policy, terms of service, or data governance documentation
- ✓ Marketing materials and pitch decks referencing your certification status
- ✓ Press releases announcing certification with the phrase "certified by ODIPA"
- ✓ Procurement responses and RFP submissions demonstrating privacy credentials
- ✓ Regulatory filings where third-party privacy assessment documentation is relevant

Prohibited Uses

- ✗ Any modification of the Trust Seal design, colors, or proportions
- ✗ Use of the Trust Seal after certification has expired or been revoked
- ✗ Claiming ODIPA certification implies regulatory compliance or legal safe harbor
- ✗ Sub-licensing the Trust Seal to subsidiaries or affiliates without separate assessment
- ✗ Use in a manner that implies ODIPA endorses your products or services generally
- ✗ Continuing to display the Trust Seal after receiving notice of revocation

Digital Trust Seal implementations must link to ODIPA's certification verification page at odipa.org/verify, where the public can confirm certification status and year.

8. PRICING & ENGAGEMENT TIERS

Certification Fees

All fees are at fair market value, applied uniformly to all applicants in each tier. Fees are not negotiated based on applicant identity or commercial interests. ODIPA's pricing reflects the cost of qualified assessor time, panel deliberation, report writing, and ongoing Trust Seal maintenance.

Tier	Scope	Initial Fee	Renewal Fee	Notes
Small Business	Under 50 employees 1–2 frameworks	**$500**	$250	Documentation review + 1-hour structured interview. Standard 5-domain assessment.
Mid-Market	50–500 employees 2–4 frameworks	**$1,500**	$750	Full documentation review + 2-hour structured interview. 5-domain assessment with deeper vendor management review.
Enterprise	500+ employees Multiple frameworks	**$3,000**	$1,500	Extended documentation review + 3-hour structured interview across multiple stakeholders. Full 5-domain assessment with sub-processor and cross-border review.
Financial Services (Any size)	GLBA, BSA, PCI DSS, CCPA, NYDFS Part 500	**$5,000**	$2,500	Specialist financial services assessors. Covers GLBA safeguards, BSA data requirements, PCI DSS scope, and applicable state laws. Includes examiner-ready documentation summary.
Healthcare (Any size)	HIPAA, HITECH, applicable state laws	**Custom**	Custom	HIPAA-specialized assessors (CHPC credential required). Contact us for scoping.
International	GDPR and/or non-U.S. frameworks	**Custom**	Custom	CIPP/E required. Multi-jurisdiction assessments scoped individually.

Payment Terms

- 50% of the initial fee is due upon execution of the Statement of Work
- Remaining 50% is due upon delivery of the Assessment Report
- Renewal fees are due prior to commencement of renewal assessment
- Re-assessment after a Not Certified outcome: 50% of initial fee

- All payments by check or ACH. ODIPA does not accept credit cards at this time

Tax Treatment

Certification fees are payments for professional services rendered — not charitable contributions. They are not deductible as charitable contributions under IRC Section 170. They may be deductible as ordinary business expenses under IRC Section 162. Consult your tax advisor regarding deductibility in your jurisdiction.

9. ANNUAL RENEWAL

Keeping Certification Current

Privacy law is a rapidly evolving field. New state laws take effect each year, existing frameworks are updated, and organizational data practices change. ODIPA's annual renewal process ensures that the Trust Seal always reflects current practices and applicable law — not a snapshot from years ago.

What triggers renewal?

Certification expires 12 months from the date of issuance. ODIPA sends a renewal reminder 90 days before expiration.

What does renewal involve?

A streamlined review of: changes to your privacy practices since last assessment, new frameworks applicable to your organization, updates to existing frameworks (e.g., new CCPA regulations), and any significant data incidents or regulatory enforcement actions.

Is a full reassessment required?

Not in most cases. Renewal is typically 40–60% of the initial assessment scope. A full reassessment may be required if: your organization has undergone a merger or acquisition, your data processing activities have materially changed, or a significant incident has occurred since last certification.

What happens if I let certification lapse?

Your Trust Seal license expires and you must cease displaying the Trust Seal immediately. Reinstatement requires a full initial assessment. ODIPA will publish the change in certification status on odipa.org/verify.

What triggers revocation?

ODIPA may revoke certification immediately if: you suffer a material data breach and fail to notify ODIPA within 14 days; you are subject to a regulatory enforcement action related to data privacy; or we determine through audit that you no longer meet certification standards.

10. IMPORTANT LIMITATIONS & DISCLAIMERS

Read This Section Carefully

Certification Is Not Legal Advice

ODIPA is a nonprofit education organization, not a law firm. Nothing in this guide or in any ODIPA assessment report constitutes legal advice, legal opinion, or regulatory guidance. ODIPA assessors are not acting as legal counsel to your organization. You should continue to work with qualified privacy counsel on your legal compliance obligations regardless of certification status.

Certification Is Not a Legal Safe Harbor

ODIPA certification does not provide immunity from regulatory enforcement, civil litigation, or any other legal action. Regulators — including the FTC, state attorneys general, and international data protection authorities — make independent enforcement determinations. ODIPA certification may be relevant evidence of good-faith compliance efforts but is not a guarantee of any outcome.

Certification Is a Point-in-Time Assessment

Your certification reflects your organization's data practices as reviewed during the assessment period. Data practices, personnel, technology, and applicable law change continuously. ODIPA is not responsible for changes to your practices or applicable law that occur after the assessment is completed.

Certification Is Not Ongoing Monitoring

ODIPA does not continuously monitor certified organizations. Between annual renewals, ODIPA has no visibility into your data practices. You are responsible for maintaining practices consistent with your certification and for notifying ODIPA of material changes.

Assessment Report Confidentiality

Your Assessment Report — including gap analysis and specific findings — is confidential. ODIPA publishes only certification status (certified / not certified) on odipa.org/verify. You are responsible for how you use and distribute your Assessment Report. ODIPA recommends treating the report as attorney-client privileged if shared with legal counsel.

AI-Assisted Development

ODIPA's assessment frameworks, documentation, and certification materials were developed with AI assistance (Claude by Anthropic). ODIPA reviews all AI-generated content for accuracy before publication. The use of AI development tools does not affect the validity, thoroughness, or independence of the assessment process.

Common Questions

Q: How long does the assessment take?

A: 4–8 weeks from signed Statement of Work to report delivery for most organizations. Small businesses can move faster (2–4 weeks). Enterprise and multi-framework assessments may take 8–12 weeks. Timeline depends on your document readiness and scheduling availability for the structured interview.

Q: Do we have to fix all gaps before certification?

A: Not necessarily. Certification requires that you meet all material requirements for the assessed frameworks. Non-material gaps generate remediation recommendations but do not prevent certification. Material gaps in critical areas (e.g., no breach notification procedure at all, no consumer rights process) will result in Not Certified or Provisional Certified outcomes.

Q: Can we be certified for just one framework?

A: Yes. You can scope your assessment to specific frameworks (e.g., CCPA/CPRA only, or HIPAA only). Your Trust Seal will reflect the scope of certification. Additional frameworks can be added in subsequent assessments.

Q: Who on our team needs to participate?

A: Typically: your Privacy Officer or Chief Privacy Officer (required), IT Security lead (required), General Counsel or outside privacy counsel (recommended), HR representative (for training documentation), and Compliance Officer if separate from Privacy Officer. Participation beyond these roles is at your discretion.

Q: Is our assessment report public?

A: No. Your Assessment Report is confidential. ODIPA publishes only your certification status and certification year on odipa.org/verify. The detailed findings, gap analysis, and specific recommendations are shared only with your organization.

Q: What happens if we have a data breach after certification?

A: You are required to notify ODIPA within 14 days of a material data breach. ODIPA will evaluate whether the breach affects your certification status. Depending on the nature and cause of the breach, ODIPA may: take no action, require an interim review, issue provisional certification, or revoke certification pending remediation.

Q: Can our competitors see our certification details?

A: No. Competitors — or anyone else — can only see that you are certified and the year of certification, via odipa.org/verify. No other information about your assessment is public.

Q: Does certification help with regulatory audits or investigations?

A: ODIPA certification may be useful evidence of a privacy compliance program and good-faith compliance efforts. Whether and how regulators consider it depends entirely on the regulatory authority and the specific enforcement context. We cannot predict or guarantee regulatory outcomes. Consult qualified legal counsel on how to present your certification in any regulatory context.

12. HOW TO APPLY

Start Your Certification Journey

Applying for ODIPA certification takes under 10 minutes. After you submit your application, your assessment team will contact you within 2 business days to schedule a scoping call and confirm the Statement of Work.

Step 1

Submit Application Online

Visit odipa.org/get-certified and complete the certification application form. You'll provide basic organizational information, your industry, estimated employee count, and the frameworks you believe apply to your organization.

Step 2

Scoping Call (30 minutes)

Your assigned assessment team lead schedules a 30-minute call to confirm scope, timeline, and pricing. You receive a formal Statement of Work for legal review. No payment is required before the scoping call.

Step 3

Sign & Pay (50% Deposit)

Review and sign the Statement of Work. Pay the 50% deposit by check or ACH to commence the assessment. Your assessors are assigned and the document portal is activated.

Step 4

Submit Documents

Upload requested documents via ODIPA's secure portal within the agreed timeline (typically 5–10 business days). Your team is available to clarify any document request questions.

Step 5

Structured Interview

Participate in your 1–3 hour structured interview with both assessors. Most organizations find the interview straightforward when documentation is prepared.

Step 6

Receive Your Report & Seal

Receive your confidential Assessment Report. If certified, activate your Trust Seal and pay the remaining 50% balance. If not certified, your detailed gap analysis gives you a clear remediation roadmap.

Apply Online	Questions?	Legal Review
odipa.org/get-certified	partnerships@odipa.org	legal@odipa.org

ODIPA Foundation is a California 501(c)(3) nonprofit organization. EIN: [Your EIN]. All certification fees fund free consumer privacy education and open-source tool development. This guide was prepared with AI assistance and is provided for informational purposes only. See Section 10 for full disclaimers.