SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

California Consumer Privacy Act as amended by the CPRA

Gap Assessment Report

California Consumer Privacy Act as amended by the CPRA

Pacific Trail Outfitters (sample)

Consumer, loyalty programme and employee data for the online store, the mobile app and 20 California stores.

ASSESSED	25 September 2026
EDITION	Civil Code 1798.100 et seq. and the regulations in force from 1 January 2026
IN SCOPE	46 requirements, 45 applicable
PROFILE	Retail and e-commerce · 50 to 249 people · California Privacy Protection Agency
PREPARED BY	Governance Docs

CONTENTS

1 Executive summary
2 Readiness by area and where the next points come from
3 Remediation plan
A About this report

Confidential. Prepared for Pacific Trail Outfitters (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Pacific Trail Outfitters (sample) stands against CCPA/CPRA

OVERALL READINESS

60.6%

Level 2 · Developing

The programme is under way, with material gaps an auditor would find.

Initial | **Developing** | Established | Audit-ready

APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
45	12	33	10

STATUS OF EVERY REQUIREMENT

Not started · Planned · Partially implemented · Implemented, not evidenced · Implemented and evidenced · Not applicable

GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
16 of 33	5 of 33	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 60.6% against CCPA/CPRA across 45 applicable controls. 12 of them are implemented and evidenced.
- Most open gaps: Requests to know, delete and correct, with 5 at 68%. Strongest area: Service providers, contractors and third parties at 94%.
- 10 controls are operating but not evidenced. Collecting their records alone lifts the score to 66.1% (+5.5 points), the cheapest gain available.
- 10 gaps are high priority (not started or only planned); 3 of them are in Applicability and governance.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	**Put an owner and date against the 3 high-priority gaps in Applicability and governance**	Compliance Lead	Privacy Program Governance Policy
2	MEDIUM	**Adopt and tailor the Consumer Rights Policy, which closes 4 open gaps**	To assign	Consumer Rights Policy
3	LOW	**Evidence the 10 controls that already operate (+5.5 points)**	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

You stand at 61% readiness with 33 open gaps, and you must first formalize program ownership and core notices.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization sits at level 2 of 4 in privacy readiness, with a 60.6% overall score and 33 open gaps. Ten gaps are high priority, primarily in consumer notices, opt-out mechanisms, and program governance. Our main exposure lies in unevidenced controls and unassigned remediation tasks that fail to meet California Privacy Protection Agency expectations. Executive management must assign operational owners and target dates to all open gaps and approve the updated privacy program governance policies this month.

WHERE YOU STAND

Your self-assessment shows an overall score of 60.6%, placing your organization at readiness level 2 of 4, named Developing. The assessment covers 46 requirements, with 45 applicable and 1 not applicable. Out of 45 applicable controls, 33 open gaps remain across the business. Ten gaps are marked as high priority. While 12 controls are implemented and evidenced, 10 are implemented without evidence, 13 are partially implemented, 5 are planned, and 5 are not started.

WHAT IT MEANS FOR THE ORGANIZATION

The pattern indicates that foundational operational practices are underway, but formal governance and public-facing accountability lag behind. Only 16 gaps have an assigned owner and only 5 have a target date. The lowest scoring areas include Notices and privacy policy at 31.3% and Opt-out of sale and sharing at 43.8%. Without complete policies and formal records, the organization faces exposure regarding general California Privacy Protection Agency expectations, especially where consumer interactions occur.

WHERE TO FOCUS FIRST

Your immediate effort must target high-priority controls that lack documentation or execution. Start by establishing program leadership and publishing updated consumer rights notices. Next, turn attention to the 10 controls that are running but lack documentation, which would raise your score to 66.1%. Finishing the 13 partially implemented controls brings your score to 80.6%. Prioritize formalizing methods for consumer requests and defining rules for financial incentive programs before tackling lower-priority tracking tasks.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Establish privacy program ownership and governance boundaries** GOV.1 Programme ownership · 1798.140(d) Applicability as a business	Unclear ownership leaves 17 gaps unassigned and weakens accountability across retail operations. Establishing governance ensures every privacy requirement has an accountable team.	Draft and approve the core privacy governance policy assigning clear functional responsibilities.	**Privacy Program Governance Policy** Comprehensive CCPA-CPRA Compliance Toolkit – 60+ Privacy Templates	30 DAYS
2	**Implement accessible request methods and notice standards** 1798.130(a)(1) Methods for submitting requests · 11 CCR 7003 Readable and accessible notices	Consumer-facing deficiencies directly affect retail shoppers exercising privacy rights. Meeting supervisory expectations requires clear, accessible methods to receive and process consumer inquiries.	Review current customer intake channels against standard intake and verification procedures.	**Consumer Rights Policy** Comprehensive CCPA-CPRA Compliance Toolkit – 60+ Privacy Templates	30 DAYS
3	**Formalize reasonable security and breach response protocols** 1798.100(e) Reasonable security · BR.1 Breach response and notification	Security controls and incident handling are critical safeguards for consumer personal data. Gaps in documented security practices expose retail consumer records during operational incidents.	Adopt a comprehensive data security policy and incident response log across IT systems.	**Data Security Policy** Comprehensive CCPA-CPRA Compliance Toolkit – 60+ Privacy Templates	60 DAYS
4	**Structure financial incentive rules and opt-out waiting periods** 1798.125(b) Financial incentives · 11 CCR 7028 Waiting before asking again	Retail loyalty programs and consumer sharing opt-outs require structured disclosures and timing controls. Omitting these safeguards risks consumer friction and regulatory scrutiny.	Complete an assessment of customer loyalty offerings using an incentive program evaluation template.	**Financial Incentive & Loyalty Program Policy** Comprehensive CCPA-CPRA Compliance Toolkit – 60+ Privacy Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Adopt the Privacy Program Governance Policy and assign owners to all 33 open gaps.
- Update consumer rights intake procedures and publish accessible consumer notices.
- Assemble evidence for the 10 controls that are currently implemented but unevidenced.

DAYS 31 TO 60

- Approve the Data Security Policy and standardize breach response notification templates.
- Complete implementation of verification procedures for consumer requests and authorized agents.
- Deploy opt-out preference signal mechanisms and update internal sharing assessment procedures.

DAYS 61 TO 90

- Document the Financial Incentive & Loyalty Program Policy for customer promotions.
- Operationalize waiting period rules for consumer opt-out requests and record retention schedules.
- Conduct required staff training for team members handling consumer privacy requests.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Applicability and governance	1 · 2 · 1 · 1	45%	3 · 0 · 1
Data inventory and purpose limitation	1 · 1 · 1 · 1	56%	1 · 1 · 1
Notices and privacy policy	1 · 1 · 2	31%	2 · 2 · 0
Requests to know, delete and correct	4 · 1 · 2	68%	0 · 4 · 1
Opt-out of sale and sharing	1 · 3 · 1	44%	1 · 3 · 0
Sensitive personal information	1 · 1	50%	1 · 0 · 1
Service providers, contractors and third parties	1 · 3	94%	0 · 0 · 1
Minors, incentives and non-discrimination	1 · 2	50%	1 · 0 · 2
Risk assessments and automated decisions	1 · 1 · 2	81%	0 · 1 · 1
Security, breaches and cybersecurity audits	1 · 1 · 1 · 1	56%	1 · 1 · 1
Training, records and assurance	1 · 1 · 2	81%	0 · 1 · 1

Not started · Planned · Partially implemented · Implemented, not evidenced · Implemented and evidenced · Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today	60.6%	
Evidence what already runs 10 requirements	66.1%	+5.5
Finish what is partly in place 13 requirements	80.6%	+14.5
Implement what is planned 5 requirements	88.9%	+8.3
Start what has not begun 5 requirements	100.0%	+11.1

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

Consumer Rights Policy	4
Privacy Notice Policy	3
Consumer Request Tracking Log & Metrics Register	3
Right to Opt-Out of Sale/Sharing Procedure (§§ 1798.120, 1798.135)	3
CCPA/CPRA Compliance Checklist	2
Privacy Program Framework	2

All of these are in the CCPA/CPRA Toolkit (63 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH **Not started · 5**

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
GOV.1	Programme ownership	Applicability and governance	To assign	Privacy Program Governance Policy · Privacy Roles & Responsibilities (RACI Matrix) +1 more
1798.140(m)	De-identified data	Data inventory and purpose limitation	HR Manager	Data Minimization Procedure · Data Collection & Purpose Limitation Policy
1798.130(a)(1)	Methods for submitting requests	Notices and privacy policy	HR Manager	Consumer Rights Policy · Consumer Request Intake & Verification Procedure
1798.125(b)	Financial incentives	Minors, incentives and non-discrimination	To assign	Notice of Financial Incentive Template · Financial Incentive & Loyalty Program Policy +1 more
1798.100(e)	Reasonable security	Security, breaches and cybersecurity audits	To assign	Data Security Policy

HIGH **Planned · 5**

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
1798.140(d)	Applicability as a business	Applicability and governance	Compliance Lead 4 Feb 2027	CCPA/CPRA Compliance Checklist · Privacy Program Framework +1 more
GOV.2	Tracking legal change	Applicability and governance	To assign	Regulatory Change Management Procedure · CCPA/CPRA Compliance Checklist
11 CCR 7003	Readable and accessible notices	Notices and privacy policy	Compliance Lead 7 Jan 2027	Privacy Notice Policy · Privacy Policy Template (Online)
11 CCR 7028	Waiting before asking again	Opt-out of sale and sharing	To assign	Right to Opt-Out of Sale/Sharing Procedure (§§ 1798.120, 1798.135)

1798.121	Right to limit use	Sensitive personal information	HR Manager 7 Jan 2027	Right to Limit Use of Sensitive PI Procedure (§ 1798.121) · Notice to Limit Use of Sensitive PI Template +1 more

MEDIUM **Partially implemented · 13**

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
1798.100(c)	Reasonably necessary and proportionate	Data inventory and purpose limitation	To assign	Data Collection & Purpose Limitation Policy · Data Minimization Procedure
1798.100(a)	Notice at collection	Notices and privacy policy	IT Manager	Notice at Collection Template · Privacy Notice Policy
1798.130(a)(5)	Online privacy policy	Notices and privacy policy	IT Manager	Privacy Policy Template (Online) · Privacy Notice Policy
11 CCR 7060	Verification	Requests to know, delete and correct	Operations Manager	Consumer Request Intake & Verification Procedure
11 CCR 7063	Authorised agents	Requests to know, delete and correct	To assign	Authorized Agent Verification Procedure
1798.110	Right to know	Requests to know, delete and correct	HR Manager	Right to Know / Access Fulfillment Procedure (§§ 1798.100, 1798.110, 1798.115) · Consumer Rights Policy
11 CCR 7004	No dark patterns	Requests to know, delete and correct	IT Manager 24 Dec 2026	Consumer Rights Policy · Privacy-by-Design & Default Procedure
1798.120	Identifying sale and sharing	Opt-out of sale and sharing	HR Manager 29 Oct 2026	Third-Party Data Sharing Assessment Procedure · Data Processing Inventory & Record of Processing Activities
11 CCR 7025	Opt-out preference signals	Opt-out of sale and sharing	Operations Manager	Right to Opt-Out of Sale/Sharing Procedure (§§ 1798.120, 1798.135) · Consumer Rights Policy
11 CCR 7026	Processing opt-outs	Opt-out of sale and sharing	Compliance Lead	Right to Opt-Out of Sale/Sharing Procedure (§§ 1798.120, 1798.135) · Consumer Request Tracking Log & Metrics Register
RSK.2	Content of risk assessments	Risk assessments and automated decisions	Risk Manager	Privacy Risk Assessment Template · Profiling Impact Assessment Template

BR.1	Breach response and notification	Security, breaches and cybersecurity audits	Operations Manager	Data Breach Response Procedure · Data Breach Notification Template +1 more
11 CCR 7100	Training for request handlers	Training, records and assurance	IT Manager	Privacy Training & Awareness Policy · Privacy Training Plan +2 more

LOW **Implemented, not evidenced · 10**

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
GOV.3	Privacy by design	Applicability and governance	To assign	Privacy-by-Design & Default Procedure · Privacy Risk Assessment Procedure
1798.100(a)(3)	Retention periods	Data inventory and purpose limitation	To assign	Data Retention & Disposal Policy · Data Retention Schedule Template
1798.105	Right to delete	Requests to know, delete and correct	To assign	Right to Delete Fulfillment Procedure (§ 1798.105) · Consumer Request Tracking Log & Metrics Register
1798.140(ae)	Identifying sensitive personal information	Sensitive personal information	To assign	Sensitive PI Inventory & Classification Matrix · Sensitive Personal Information Policy
1798.100(d)	Contracts with every recipient	Service providers, contractors and third parties	To assign	Service Provider & Contractor Management Policy · Service Provider Agreement Template +1 more
1798.120(c)	Consumers under 16	Minors, incentives and non-discrimination	To assign	Children & Minors Privacy Policy · Age Verification & Parental Consent Procedure +1 more
1798.125(a)	Non-discrimination	Minors, incentives and non-discrimination	To assign	Non-Discrimination Compliance Procedure
RSK.3	Submissions to the CPPA	Risk assessments and automated decisions	To assign	Privacy Risk Assessment Procedure · Audit Findings & Corrective Action Register
AUD.1	Cybersecurity audit	Security, breaches and cybersecurity audits	To assign	Cybersecurity Audit Policy · Cybersecurity Audit Procedure & Checklist

11 CCR 7101	Request records	Training, records and assurance	To assign	Consumer Request Tracking Log & Metrics Register

A · ABOUT THIS REPORT

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
Not started	0.00	No policy, process or activity exists for this requirement.
Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 · Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 · Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 · Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 · Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com