Cookie Consent, GPC and Website Tracking Governance

BDC-OPS-003 | Consolidated case study v1.1 | 15 November 2026

Prepared by Olumuyiwa Michael, CIPP/US, CIPP/EU, CIPM, AIGP, CompTIA Security+

Published by BloomDale Capital LLC • Fictional enterprise: Meridian Digital Holdings • Scope: consent banner, preference center, opt-out preference signals (GPC), tracker inventory and website testing

SIMULATION DISCLOSURE Meridian Digital Holdings, its vendors, trackers, risks and findings are fictional. The prototype test results in section 7 are real runs against a controlled demonstration page, not against any production website. Nothing here is legal advice. Legal references were reviewed as of 15 November 2026. OneTrust and other consent platforms are trademarks of their owners; the prototype is an original design and implies no affiliation.

1. Executive brief

Decision: production HOLD. This package designs and tests how Meridian collects consent and honors opt-outs on its websites in the UK, the EEA, California, Connecticut and Texas. It responds to BDC-PRIV-001 finding US-F01 / GC-F02 (16, High), where opt-out signals were honored on some websites but not passed to advertising partners, and it supplies the consent and withdrawal evidence that BDC-OPS-002 requires before AI-06 can launch.

The browser-side design works: a prototype passed all 15 automated checks, and each of four planted defects was caught. That does not cover the US-F01 failure itself, which happens on the server when opt-outs are passed to ad partners; a browser prototype cannot show it, and no Meridian site has been tested. Three Critical risks remain open.

Measure, 15 November 2026	Current state
Prototype checks passed	15 of 15 (automated Chromium tests)
Controls demonstrated in prototype	7 of 11
Controls verified on a Meridian site	0 of 11
Production tests executed	0 of 16
Trackers inventoried	12 (3 under review, 1 marked for removal)
Inherent risks	11: 3 Critical, 3 High, 5 Moderate
Production release	HOLD

2. Scope and links to the portfolio

Element	Scope
Websites	Digital Platforms (advertising-supported services) and Digital Learning (online courses) public sites; HealthTech patient portal (authenticated pages); Financial Services loan application pages
Visitors	UK and EEA visitors; consumers in California, Connecticut and Texas. Colorado, Virginia, Oregon, New Jersey and Maryland are out of scope for Meridian under the BDC-PRIV-001 applicability screening
Origin	BDC-PRIV-001 finding US-F01 / GC-F02: GPC honored on some websites but not passed to downstream ad-tech partners. Risk R03 carries it forward
Dependency	BDC-OPS-002 controls PBD-01 (consent banner and withdrawal test) and PBD-04 (withdrawal reaching the pipeline) for AI-06 rely on CMP-01, CMP-03 and CMP-05 here. The AI-06 event tag is tracker TRK-010
Related process	Opt-out and deletion requests submitted through the rights channel are handled under BDC-OPS-001; this package covers opt-outs expressed on the website and through browser signals

3. Legal requirements by region

The UK and EEA require consent before non-exempt storage or access on a device. The three U.S. states allow most tracking with notice but give consumers an opt-out that browsers can exercise automatically.

Region	What the site must do	Source
EEA	Consent before any non-essential storage or access, including analytics. Consent must be specific, informed and unambiguous; pre-ticked boxes are not consent. Withdrawal must be as easy as giving consent.	ePrivacy Directive Art 5(3); GDPR Art 4(11), 7; Planet49 (C-673/17)
United Kingdom	Consent remains the rule, but since 5 February 2026 PECR Schedule A1 exempts some uses, each only for its sole purpose: statistics used to improve the service, and storage that adapts appearance or function to the visitor's own preferences. The visitor must get clear information and a simple way to object. An analytics vendor can be used under the statistics exception only as a processor helping Meridian improve its own service; a vendor that uses the data for its own purposes, advertising and profiling all still need consent. Maximum PECR penalty raised to £17.5 million or 4% of global turnover, whichever is higher.	PECR reg 6 and Sch A1, as amended by the Data (Use and Access) Act 2025; ICO storage and access technologies guidance, April 2026
California	Honor a valid opt-out preference signal such as GPC as a request to opt out of sale and sharing, for the browser and for any known account. Under the regulations as amended from 1 January 2026, the site must display whether it processed the signal or opt-out request, for example "Opt-Out Request Honored". Provide a "Do Not Sell or Share My Personal Information" link or an alternative opt-out link. Choice design must avoid dark patterns.	Cal. Civ. Code §1798.120, 1798.135; CCPA regs §7004, 7025(c)(6), 7026 (effective 1 Jan 2026)

Region	What the site must do	Source
Connecticut, Texas	Honor universal opt-out mechanisms such as GPC for sale and targeted advertising (both since 1 January 2025). Provide a clear opt-out method in the privacy notice. Opt-in consent for sensitive data. Texas exempts GLBA financial institutions and HIPAA covered entities and business associates, and Connecticut narrowed its GLBA exemption from 1 July 2026 (SB 1295); Meridian applies the same opt-out handling on HealthTech and Financial Services pages as a policy choice.	CTDPA as amended by SB 1295; TDPSA §541.002, §541.055(e)
HealthTech portal	Meridian HealthTech is a HIPAA business associate. Tracking technology on authenticated portal pages can disclose PHI to the tracking vendor, which is not permitted without a subcontractor BAA and a permitted use; a marketing use would also need patient authorization. HHS OCR guidance on online tracking still applies to authenticated pages. In June 2024 a federal court vacated only the part covering an IP address combined with a visit to an unauthenticated page, and HHS dropped its appeal.	45 CFR 164.502(e), 164.508(a)(3); HHS OCR tracking bulletin; AHA v. Becerra (N.D. Tex. 2024)

4. Consent and choice design

Figure 1 shows the decision logic applied on every page view. Two rules hold across regions: a GPC signal always turns advertising off, and when the visitor's location is unknown the site applies the EEA consent rules, the strictest set.

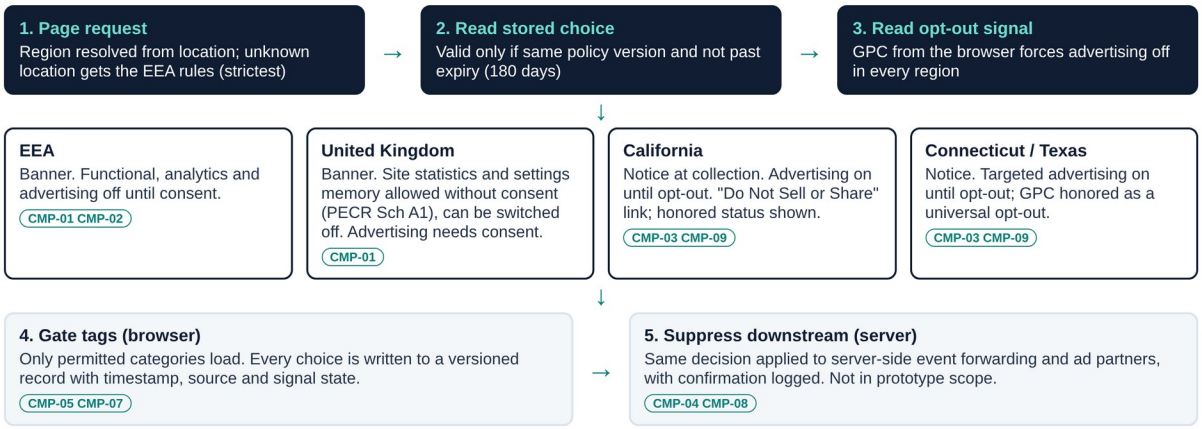


Figure 1. Consent and opt-out decision logic with control IDs. Original illustration.

Category treatment

Category	EEA	UK	California, Connecticut, Texas
Strictly necessary	Always on	Always on	Always on
Functional	Off until consent	Settings memory on once the visitor sets a preference, can be switched off (Sch A1); other functional tools need consent	On with notice
Analytics	Off until consent	Statistics used only to improve the site (Meridian or its processor) on, can be switched off; vendors using data for their own purposes off until consent	On with notice
Advertising	Off until consent	Off until consent	On until opt-out or GPC

Design rules

- Accept all, Reject all and Manage preferences use identical styling and appear together on the first layer, so refusing takes no more effort than accepting and no option is visually favored.
- Before a choice, the browser holds only the strictly necessary session value. Nothing optional, including the demonstration's own event log, is stored until the visitor chooses.
- Nothing is pre-ticked where consent is the rule. The preference center explains the rule that applies in the visitor's region next to each switch.
- A persistent "Your Privacy Choices" link reopens the preference center, so withdrawal takes the same number of steps as consent.
- When GPC is present the advertising switch is locked off and the page says why. A visitor who wants advertising must turn the signal off in the browser; the site does not ask them to override it.
- Each saved choice records region, choices, source, policy version, timestamp, expiry and whether a signal was present (simulated or from the browser). Records expire after 180 days, a Meridian policy choice. A new policy version, an unreadable date or a damaged record means the choice is asked for again. If the browser blocks storage, the visitor is told the choice applies to this page only.

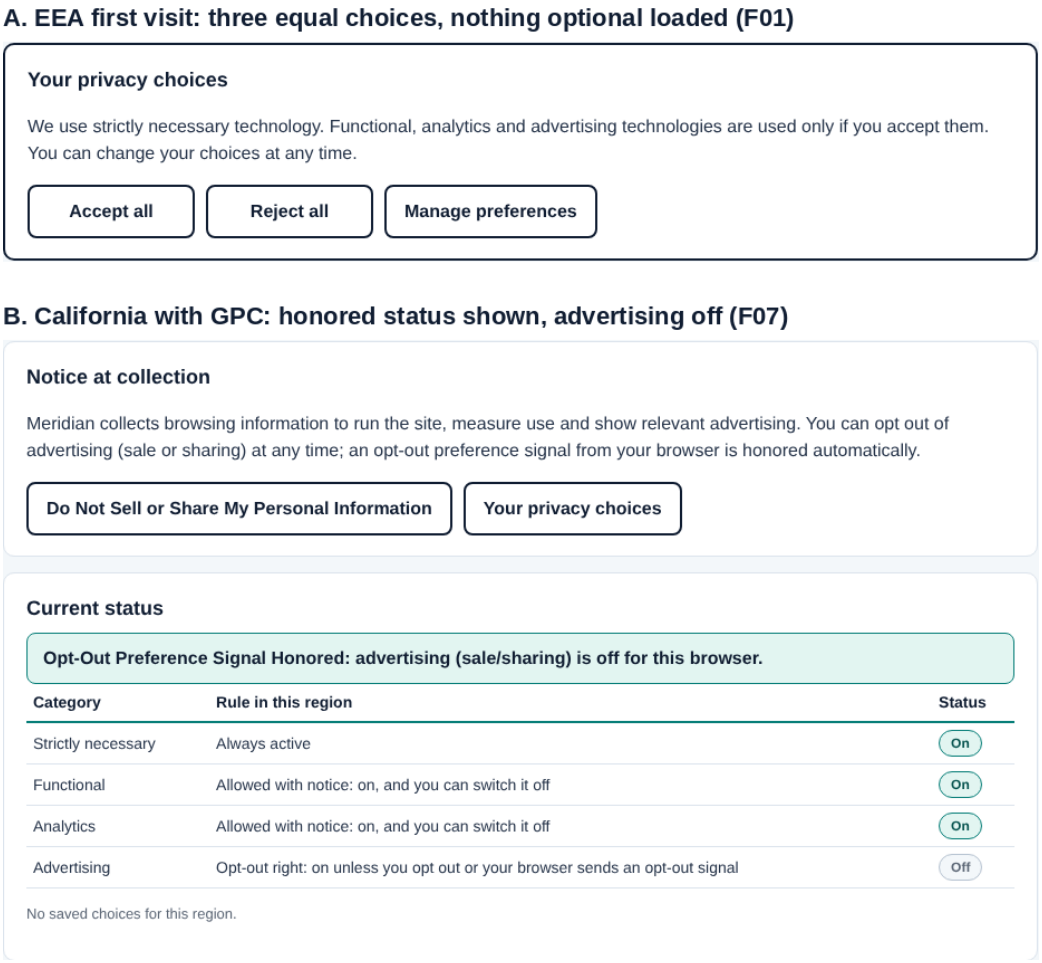


Figure 2. Prototype screens captured during automated tests F01 and F07.

5. Tracker inventory

The workbook holds a synthetic inventory of 12 tracking technologies, each with a TRK ID, owner, purpose, category, legal basis by region, retention and classification status. Four exist in the prototype as harmless mocks (TRK-001 to TRK-004). Three entries carry most of the risk:

ID	Technology	Why it matters
TRK-006	Third-party analytics suite (Digital Learning)	The vendor may use the data for its own purposes, so the UK statistics exemption does not apply. Needs consent in the UK and EEA, and its contract must be reviewed for CCPA sale or sharing (R04).
TRK-010	AI-06 personalization event tag	Profiling falls outside every PECR exemption, so it needs consent in the UK and EEA. In Connecticut and Texas, use limited to Meridian's own sites is not targeted advertising. Linked to BDC-OPS-002 PBD-01 and PBD-04 (R10).
TRK-012	Marketing pixel on patient portal	Found on authenticated HealthTech pages with no BAA in place. Marked for removal (R09, Critical).

6. Testing methodology

Website testing follows nine repeatable steps. Automated scans are discovery inputs: a cookie appearing in a scan is not a legal finding until it is reconciled to the inventory and reviewed.

Step	Name	What is done
S01	Baseline	Clean browser profile; record cookies, local storage, scripts, pixels and third-party requests before any interaction
S02	Reject	Reject optional tracking, reload and compare against baseline
S03	Selective	Allow analytics only; confirm advertising stays blocked where consent is required
S04	Accept	Accept all and record which trackers and recipients activate
S05	Withdraw	Withdraw consent, reload and confirm optional requests stop. Data already collected is a separate issue
S06	Signal	Repeat with GPC on and off; check the opt-out outcome, not just the banner
S07	Geography	Run each regional scenario and compare banners, defaults, links and opt-out behavior. Confirm the site actually switched rule sets; a VPN alone proves nothing
S08	Reconcile	Map every observation to a TRK ID, vendor contract, purpose and legal rule
S09	Triage	Assign severity, owner, due date and corrective action; retest after the fix

Each observation is recorded with a scan ID, environment, region, browser state, technology, tracker ID (or UNCLASSIFIED), request domain, consent event, observed behavior, legal assessment and finding status. No test is marked Pass without an evidence artifact and reviewer sign-off.

Two tiers of evidence. Prototype results come from real test runs against a controlled page. Production tests T01 to T16 describe what must run on Meridian's sites and stay "Not executed" in the workbook. The workbook never turns prototype results into a production pass rate.

7. Prototype test results

On 15 November 2026 the prototype was tested in headless Chromium using Playwright, with a fresh browser profile for each check. Mock analytics and advertising tags send requests to domains under the reserved .invalid top-level domain, which cannot resolve, so the network log shows exactly which tags fired without any data leaving the browser. GPC was simulated through a URL parameter because headless browsers do not send the signal. On a real visit the page reads the browser's navigator.globalPrivacyControl property; a production site would also read the Sec-GPC request header on the server.

ID	Check	Region	Evidence	Result
F01	First visit: banner shown, no optional requests or storage	EEA	No requests; session key only	Pass
F02	Reject all blocks optional trackers and persists after reload	EEA	No requests after reload	Pass

ID	Check	Region	Evidence	Result
F03	Accept all fires analytics and advertising	EEA	Both mock hosts called	Pass
F04	Analytics-only choice: analytics fires, advertising does not	EEA	Analytics host only	Pass
F05	Withdrawal from footer link stops trackers on next page view	EEA	No requests on final view	Pass
F06	First-party statistics on, advertising off before any choice	UK	Analytics host only	Pass
F07	GPC: advertising off and "Signal Honored" shown	California	Status text; no ad host	Pass
F08	No GPC: notice and "Do Not Sell or Share" link shown	California	Link visible	Pass
F09	Link opts out and shows "Opt-Out Request Honored"	California	No ad host on final view	Pass
F10	GPC: targeted advertising off	CT / TX	No ad host	Pass
F11	GPC overrides Accept all for advertising	EEA	Advertising off	Pass
F12	Expired choice brings the banner back and blocks trackers	EEA	Banner visible	Pass
F13	Accept, Reject and Manage have identical computed styles	EEA	Styles match	Pass
F14	Unreadable expiry date treated as expired	EEA	Banner back; no requests	Pass
F15	Damaged saved record discarded without breaking the page	EEA	Banner back; no requests	Pass

Do the tests catch failures? tests/mutation_check.py plants four defects in copies of the page: Reject all leaving advertising on, the GPC check removed, the Accept button given a filled navy style, and an expiry check that accepts unreadable dates. The suite fails on each: at F02; at F07, F10 and F11; at F13; and at F14. Anyone can rerun both scripts. Screenshots for every check are in the evidence folder.

What these results do not show. They do not show server-side suppression, vendor syncs, real geolocation, authenticated portal pages or behavior on any Meridian site. Those are covered by production tests T05, T09, T10, T11 and T13, none of which has run.

8. Risk register

Scores are likelihood × impact on 1–5 scales, using the portfolio bands: Low 1–5, Moderate 6–12, High 13–19, Critical 20–25. Target scores assume the linked controls are verified in production; they are estimates, not evidence.

ID	Risk	Inherent	Target	Controls
R01	GPC ignored on the website	4 × 5 = 20 Critical	2 × 4 = 8 Moderate	CMP-03, CMP-09

ID	Risk	Inherent	Target	Controls
R02	Non-exempt trackers fire before a UK/EEA choice	4 × 5 = 20 Critical	2 × 4 = 8 Moderate	CMP-01, CMP-02
R09	Third-party pixel on HealthTech portal discloses PHI without a BAA	4 × 5 = 20 Critical	1 × 5 = 5 Low	CMP-10
R03	Opt-outs not passed to ad partners or server-side forwarding (US-F01)	4 × 4 = 16 High	2 × 4 = 8 Moderate	CMP-04, CMP-08
R04	Third-party analytics treated as exempt UK statistics	4 × 4 = 16 High	2 × 3 = 6 Moderate	CMP-06
R10	AI-06 tag collects events without consent or after opt-out	3 × 5 = 15 High	1 × 5 = 5 Low	CMP-01, CMP-03, CMP-05
R05	Withdrawal not applied downstream	3 × 4 = 12 Moderate	2 × 3 = 6 Moderate	CMP-05, CMP-04
R06	Vendor opt-out sync failures unnoticed	3 × 4 = 12 Moderate	2 × 3 = 6 Moderate	CMP-08
R07	Visitor routed to the wrong rule set	3 × 4 = 12 Moderate	2 × 3 = 6 Moderate	CMP-01
R11	Banner nudges toward Accept	3 × 4 = 12 Moderate	1 × 4 = 4 Low	CMP-11
R08	Consent records lack version, expiry or audit data	3 × 3 = 9 Moderate	1 × 3 = 3 Low	CMP-07

9. Release gates and monitoring

Production release requires all of the following. The workbook's Summary sheet has a Y/N cell for each gate and calculates the decision: it shows HOLD until every gate is Y, every production test has passed, every control is verified in production and no Critical risk is open.

1. TRK-012 removed from the patient portal and T13 passed on authenticated pages.
2. Production tests T01 to T16 executed on a staging copy of each Meridian site, with evidence and reviewer sign-off.
3. Server-side suppression (CMP-04) shown end to end: a GPC or opt-out stops TRK-005 conversion events, and partner confirmations are logged (T05, T09, T11). This closes the evidence gap behind BDC-PRIV-001 finding US-F01.
4. Contracts for TRK-006, TRK-007 and TRK-011 reviewed, and each tracker classified.
5. Legal sign-off on the UK statistics exemption for TRK-003 and the CCPA treatment of each vendor.

Once live, seven KPIs (M01 to M07 in the workbook) track pre-choice blocking, signal enforcement, the unclassified tracker backlog, failed downstream suppressions, open Critical and High risks, withdrawal success and third-party requests on portal pages.

10. Limitations

- A browser prototype cannot prove what happens on servers or at vendors. Real verification needs staging sites, live tags and partner-side logs.
- GPC was simulated, and region was set by URL rather than by geolocation.
- Storing choices in browser local storage is fine for a demonstration but is not an enterprise consent record. Production needs a server-side record keyed to the consent event.
- The UK rules are new. The ICO's April 2026 guidance reads the statistics exemption narrowly, and the ICO has advised government on further changes for online advertising, so the UK rule set should be reviewed each quarter.
- Legal conclusions are for a fictional company and would be confirmed by counsel for a real one.

11. Package contents

File	Purpose
BDC-OPS-003_Consolidated_Consent_Tracking_Case_Study_v1.1 (.docx, .pdf)	This document
BDC-OPS-003_Consent_Compliance_Workbook_v1.1.xlsx	Summary, control catalog, tracker inventory, test matrix, prototype results, risk register, monitoring plan, method and sources
BDC-OPS-003_Consent_Prototype_v1.1.html	Self-contained prototype; open in any browser or publish on GitHub Pages
evidence/ (15 PNG files and fixture_results.json)	Screenshots and raw results for F01 to F15
tests/run_tests.py, tests/mutation_check.py	Playwright test script and planted-defect check (run from the package root; needs Python and Playwright)

Sources

- CCPA regulations effective 1 January 2026 (CPPA): https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf
- California Privacy Protection Agency, regulations page: https://cppa.ca.gov/regulations/
- ICO guidance on storage and access technologies: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/
- Data (Use and Access) Act 2025: https://www.legislation.gov.uk/ukpga/2025/18
- Texas Business and Commerce Code ch. 541 (TDPSA): https://statutes.capitol.texas.gov/Docs/BC/htm/BC.541.htm
- Connecticut Attorney General, CTDPA: https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act
- HHS OCR, use of online tracking technologies: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
- Global Privacy Control specification (W3C draft): https://www.w3.org/TR/2025/WD-gpc-20250710/
- Global Privacy Control project: https://globalprivacycontrol.org/

About the author

Olumuyiwa Michael, CIPP/US, CIPP/EU, CIPM, AIGP, CompTIA Security+

Privacy and compliance professional with more than seven years of experience in privacy operations, privacy impact assessments, data subject rights, incident management and regulatory compliance, and a technical background in database administration and information security.