Enterprise PIA/DPIA & Privacy by Design

BDC-OPS-002 | Consolidated case study and executive decision pack v1.2 | 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 • System: AI-06 Customer Personalization Platform (Digital Platforms) • Assessment ID: MDH-DPIA-2026-01

SIMULATION DISCLOSURE All organizations, datasets, owners, risks, actions, decisions and workflow states are fictional. This document demonstrates a proposed governance approach; it is not evidence of a deployed system, real control tests or legal advice. Legal references were reviewed as of 15 November 2026. OneTrust is a trademark of its owner; no affiliation, sponsorship or endorsement is implied.

1. Executive decision brief

Decision: production HOLD. AI-06 would deliver personalized product and content recommendations on Meridian's own websites and app, using segmentation and propensity scoring. A DPIA is required, one inherent risk is Critical and six are High, and none of the required controls has yet been verified. The platform cannot be released until the evidence gates in section 8 are passed.

Executive measure, 15 November 2026	Current state
Inherent risks	8: 1 Critical, 6 High, 1 Moderate
Risk actions at P0	6 of 8
AI-specific Privacy by Design controls	10: 8 at P0, 2 at P1
Verified control evidence	0
Validated residual risk scores	0 of 8
Risk actions complete	0 of 8
Production release	HOLD

Target scores in section 5 are modeled post-mitigation estimates, not evidence of risk reduction. Risk actions and controls are counted separately: eight risk actions are tracked in the register, and ten controls address them.

2. System and processing description

AI-06 is a new entry in the AI system inventory of BDC-PRIV-001, owned by Meridian's Digital Platforms business. Meridian acts as controller for all processing described here.

Element	Description
Controller	Meridian Digital Holdings, Inc., a U.S. controller with no EU or UK establishment. Subject to EU and UK GDPR under Article 3(2); Article 27 representatives appointed in the EU and UK
Purpose	Personalized product and content recommendations on Meridian's own websites and app, through customer segments and propensity scores
Data subjects	Digital Platforms customers and signed-in visitors in the United States, EU and UK. Accounts of people under 18 are excluded from profiling and receive contextual recommendations only
Data categories	Website and app events (clickstream), CRM preferences, Digital Platforms purchase history, email engagement signals
Excluded by design	Special category and sensitive data; inferred sensitive traits; Meridian HealthTech PHI; Meridian Financial Services customer data (GLBA); precise geolocation
Recipients	Internal Digital Platforms product and marketing teams; U.S. cloud hosting processor. No sale; no cross-context behavioral advertising at current scope
Retention (proposed)	Raw events 90 days; derived features 12 months; audit logs per the retention schedule
Transfers	Data collected directly from EU and UK users by a U.S. controller is not a Chapter V transfer (EDPB Guidelines 05/2021). Onward transfers by any EU or UK sub-processor use the EU-U.S. Data Privacy Framework or SCCs (EU data) and the UK Extension to the DPF, IDTA or UK Addendum (UK data)
Outside scope	Credit, pricing, eligibility or any other decision with legal or similarly significant effects

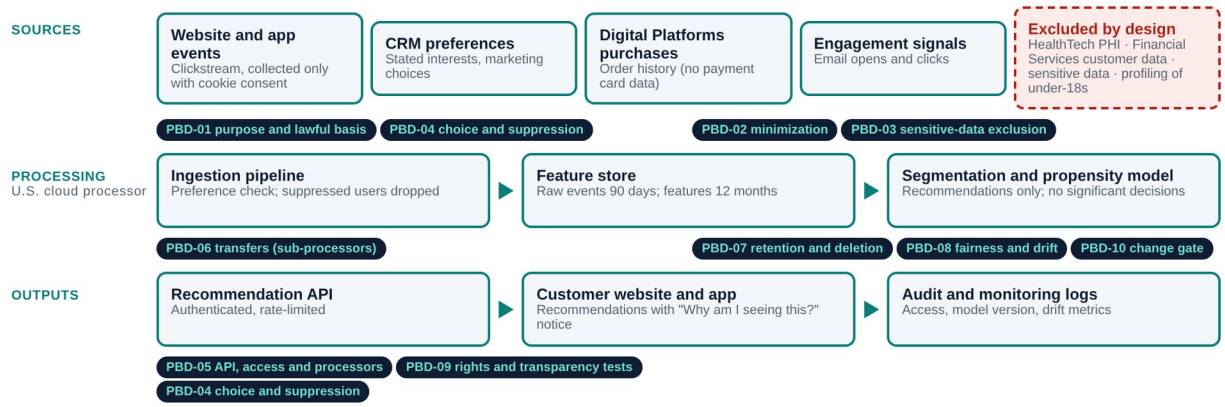


Figure 1. AI-06 data flow with Privacy by Design control points. Original illustration.

3. Legal screening and conclusions

Conclusions for this fictional scenario, using the applicability screening in BDC-PRIV-001.

Area	Conclusion	Controls
DPIA requirement (EU and UK GDPR)	Required. Not under Article 35(3)(a), because recommendations have no legal or similarly significant effects, but because the processing meets four WP248 criteria (evaluation or scoring, large-scale processing, combining datasets, innovative technology) and falls on the ICO's list (innovative technology, large-scale profiling, data matching, online tracking).	All

Area	Conclusion	Controls
Lawful basis and cookies	Collecting website and app events through non-essential cookies or similar tracking needs consent under ePrivacy Directive Article 5(3) and UK PECR regulation 6; the same applies to email open-tracking pixels. The analytics and functionality exemptions added to PECR by the Data (Use and Access) Act 2025 do not cover behavioral profiling. Profiling built on that data relies on consent; CRM-preference data may use legitimate interests with a documented balancing test.	PBD-01, PBD-04
Transparency, withdrawal and objection	Profiling is explained in privacy notices (Articles 13–14) and at the point of recommendation. For consent-based profiling, withdrawing consent must be as easy as giving it and stops profiling (Article 7(3)). For legitimate-interests segments, the right to object to profiling for direct marketing is absolute (Article 21(2)–(3)). Article 22, and UK Articles 22A–22D, are not engaged because no significant decisions are made.	PBD-04, PBD-09
U.S. state laws	California, Connecticut and Texas are in scope. Under the CTDPA and TDPSA, recommendations based on activity within the controller's own sites and apps are not "targeted advertising". Under the CCPA no "sharing" occurs: AI-06 uses only Digital Platforms first-party data, discloses it only to service providers under CCPA-compliant contracts, and uses no third-party tags or data from Meridian's other brands. Connecticut and Texas require a data protection assessment, weighing benefits against risks and safeguards, for profiling that presents a reasonably foreseeable risk of harm; this DPIA is designed to serve as that assessment. If data were used for cross-site advertising, opt-outs, GPC and a CCPA risk assessment would apply. Connecticut now protects minors aged 13 to 17 and bars design features that increase a minor's use of an online service, so under-18 accounts are excluded from profiling.	PBD-01, PBD-03, PBD-10
California ADMT and risk assessments	Not triggered. ADMT duties (from 1 January 2027) cover significant decisions such as lending, housing, education, employment and healthcare; product recommendations are not one. None of the CCPA risk-assessment triggers applies: no selling or sharing, no sensitive personal information and no ADMT for significant decisions.	PBD-10
EU AI Act and Colorado	Not high-risk: recommender systems are not listed in Annex III (Annex III duties apply from 2 December 2027 under Regulation (EU) 2026/1744). Article 5 screening completed: no manipulative techniques and no exploitation of age or other vulnerabilities. AI-literacy measures apply to the teams operating AI-06. Colorado SB 26-189 covers consequential decisions only. Any expansion toward significant decisions triggers reassessment (risk R08).	PBD-03, PBD-10
HIPAA and GLBA	Not applicable by design: HealthTech PHI and Financial Services customer data are excluded from the feature store, and the exclusion is tested.	PBD-02, PBD-03
International transfers	Direct collection by a U.S. controller is not a Chapter V transfer, but any onward transfer from an EU or UK sub-processor needs a mechanism: DPF or SCCs for EU data; UK Extension to the DPF, IDTA or UK Addendum for UK data. The DPF faces a pending appeal at the CJEU, so SCCs are kept ready as a fallback.	PBD-06
Prior consultation (Article 36)	Required only if the DPIA shows a high risk that measures cannot sufficiently reduce. Decided at the residual-risk gate.	Gate 6

4. Necessity, proportionality and consultation

Necessity (Article 35(7)(b)): Meridian's goal is relevant recommendations that reduce search effort and return rates. Three options were compared.

Option	Privacy impact	Outcome
A. Contextual recommendations (current page only)	No profile; no tracking beyond the session	Default for visitors without consent
B. Segment-level personalization	Coarse segments from CRM preferences	Fallback if consent rates are low
C. Individual propensity scoring	Behavioral profile across sources	Only with consent, excluded data removed, 90-day raw retention

Proportionality: option C is limited by minimization (PBD-02), sensitive-data exclusion (PBD-03), retention caps (PBD-07) and an always-available objection route (PBD-04).

DPO advice (Article 35(2)): the fictional Data Protection Officer reviewed the draft DPIA and advised consent-based event collection, exclusion of sensitive inferences and a 90-day cap on raw events. All three were adopted.

Data subjects' views (Article 35(9)): Article 35(9) applies where appropriate, and Meridian has chosen to seek views through a preference-center usability study with Digital Platforms customers before launch. Pending; required at the rights gate.

5. Risk register

Inherent score = likelihood × impact (1 to 25), banded as in BDC-PRIV-001: Low 1–5, Moderate 6–12, High 13–19, Critical 20–25.

ID	Potential harm	Inherent (L × I)	Target* (L × I)	Priority	Controls	Owner
R01	Unexpected behavioral profiling; loss of autonomy	4 × 4 = 16 High	2 × 3 = 6 Moderate	P0	01, 02, 04, 09	Privacy Office
R02	Sensitive inference or discriminatory targeting	4 × 5 = 20 Critical	2 × 4 = 8 Moderate	P0	03, 08	AI Governance
R03	Unauthorized disclosure via processor or API	3 × 5 = 15 High	2 × 4 = 8 Moderate	P0	05	Information Security
R04	Over-retention and repurposing of clickstream	4 × 4 = 16 High	2 × 3 = 6 Moderate	P1	01, 02, 07	Data Platform Owner
R05	Objection or deletion requests not propagated	4 × 4 = 16 High	2 × 3 = 6 Moderate	P0	04, 07, 09	Privacy Operations
R06	Cross-border transfer without valid safeguards	3 × 5 = 15 High	2 × 4 = 8 Moderate	P0	06	Privacy Legal
R07	Model drift produces misleading or unfair recommendations	3 × 4 = 12 Moderate	2 × 3 = 6 Moderate	P1	08, 10	AI Governance
R08	Unapproved expansion to significant automated decisions	3 × 5 = 15 High	1 × 5 = 5 Low	P0	01, 03, 10	Business Risk Owner

**Target is a modeled estimate, not a validated residual score. All eight risks have no verified evidence and no validated residual score.*

Why R04 is P1 despite a High score: its pre-release elements, the 90-day cap on raw events and purpose limitation against repurposing, are verified under P0 controls PBD-02 and PBD-01. No derived feature can reach its 12-month limit before PBD-07's scheduled deletion goes live within 60 days of launch. Request-driven erasure across raw events, derived features and segments is verified before release under PBD-09.

Why PBD-08 is P1 although it addresses R02: R02 is mitigated before release by PBD-03 (P0), which removes sensitive features and includes a pre-launch bias test using proxy analysis on a labeled hold-out sample. PBD-08 adds ongoing fairness and drift monitoring, which needs production data.

ID	Risk	Inherent	Priority	PBD-01 P0	PBD-02 P0	PBD-03 P0	PBD-04 P0	PBD-05 P0	PBD-06 P0	PBD-07 P1	PBD-08 P1	PBD-09 P0	PBD-10 P0
R01	Unexpected behavioral profiling	16 · High	P0	●	●		●					●	
R02	Sensitive inference or discriminatory targeting	20 · Critical	P0			●					●		
R03	Unauthorized disclosure via processor or API	15 · High	P0					●					
R04	Over-retention and repurposing of clickstream	16 · High	P1	●	●					●			
R05	Objection or deletion not propagated	16 · High	P0				●			●		●	
R06	Transfer without valid safeguards	15 · High	P0						●				
R07	Model drift; misleading or unfair recommendations	12 · Moderate	P1								●		●
R08	Expansion to significant automated decisions	15 · High	P0	●		●							●

● control mitigates the risk · Inherent score = likelihood × impact (1–25): Low 1–5, Moderate 6–12, High 13–19, Critical 20–25 · Every risk maps to at least one P0 control

Figure 2. Risk-to-control matrix. Every risk maps to at least one P0 control.

6. Privacy by Design controls

Ten AI-specific controls, specified in companion deliverable BDC-OPS-002B, sit on top of the 12 enterprise baseline controls in BDC-OPS-002A.

Control	Risks	Priority	Evidence required before release
PBD-01 Purpose and lawful basis	R01, R04, R08	P0	Approved lawful-basis record; purpose-limitation rule; consent banner and withdrawal test
PBD-02 Data and feature minimization	R01, R04	P0	Feature list review; 90-day raw-event cap configuration; PHI and GLBA field-exclusion test
PBD-03 Sensitive inference and automation restriction	R02, R08	P0	Sensitive-attribute exclusion test; pre-launch bias test; use-case restriction in model card
PBD-04 Choice and suppression propagation	R01, R05	P0	End-to-end test of consent withdrawal and objection reaching the pipeline
PBD-05 API, access and processor safeguards	R03	P0	API access review; penetration test summary; processor due diligence; Article 28 and CCPA service-provider contract
PBD-06 Transfer safeguards	R06	P0	Transfer map of sub-processors; DPF or UK Extension certification check, or executed SCCs, IDTA or UK Addendum; transfer risk assessment
PBD-07 Retention and deletion lifecycle	R04, R05	P1	Deletion job logs; feature-store retention report
PBD-08 Fairness, accuracy and drift	R02, R07	P1	Monthly fairness and drift report with thresholds
PBD-09 Rights and transparency tests	R01, R05	P0	Notice review; access, deletion and objection test cases run through the BDC-OPS-001 DSAR process
PBD-10 Change and reassessment gate	R07, R08	P0	Change triggers in release process; reassessment record

P1 does not mean optional: a P1 control becomes a release blocker if the law, the DPIA decision or an unacceptable risk requires it.

7. Assessment workflow

Stage	Deliverable
1 Intake	Initiative, purposes, datasets, jurisdictions and vendors
2 Screen	15 screening questions; DPIA determination and routing
3 Assess	DPIA, data flow, risks R01–R08 and legal review
4 Remediate	PBD-01 to PBD-10 assigned with owners, deadlines and expected evidence
5 Validate	Independent testing; residual scores only after tests
6 Decide	Privacy, Legal, Security, AI governance and risk-owner decisions recorded
7 Release or hold	Release only when every mandatory gate passes
8 Monitor	Reassess on material change, incidents or drift

The workflow is designed to run in a privacy management platform such as OneTrust. It is an original conceptual mapping, not a description of OneTrust's licensed features, screens or automation rules.

8. Release gates and decision log

Gate	Required evidence	Status	Owner
1 Purpose and lawful basis	Approved jurisdictional analysis, consent design and notices	Pending	Privacy Legal
2 Mandatory P0 controls	Independent test results for eight P0 controls	Not started	Privacy Engineering
3 Rights and preferences	End-to-end consent, objection and DSAR tests; data-subject views	Not started	Privacy Operations
4 Security and vendors	API and access tests; processor due diligence	Not started	Information Security
5 Transfers	Transfer map, mechanism and transfer risk assessment	Pending	Privacy Legal
6 Residual risk	Validated residual scores; Article 36 decision if high risk cannot be sufficiently reduced	Not assessed	Privacy Office
7 Formal approval	Signed Privacy, Legal, Security, AI governance and risk-owner record; DPO sign-off on residual risk	Not signed	Business Risk Owner

Decision log, 13 November 2026: production HOLD recorded by the Business Risk Owner, Digital Platforms (fictional). No risk acceptance can override applicable law. Any High or Critical residual risk that remains after validation is escalated. If the DPIA shows a high risk that measures cannot sufficiently reduce, Meridian will consult the competent supervisory authorities (no lead authority applies without an EU establishment) and the ICO under Article 36 before release. The internal High and Critical bands are a proxy for, not the same as, the GDPR high-risk test. The DPIA is reviewed at least annually and on any material change (Article 35(11)).

9. Limitations

- All organizations, data, owners and decisions are synthetic. Scores and targets illustrate the method; they are not evidence.
- Legal conclusions apply to this fictional scenario as of 15 November 2026 and are not legal advice.
- OneTrust is referenced as an example platform; the study does not represent a configured tenant, an endorsement or an affiliation.

10. Companion deliverables

- **BDC-OPS-002A**: Enterprise Privacy by Design master checklist (12 baseline controls with industry overlays).
- **BDC-OPS-002B**: AI-specific Privacy by Design controls PBD-01 to PBD-10 and the risk crosswalk.
- **BDC-OPS-002 Executive Dashboard**: one-page decision summary for leadership.
- **BDC-PRIV-001**: enterprise assessment that sets Meridian’s profile and applicability screening; AI-06 joins its AI system inventory.
- **BDC-OPS-001**: DSAR operations, used to test rights handling under PBD-09.

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.

This case study is part of the BloomDale Capital LLC Data Privacy & AI Governance Portfolio: https://mikeolu700-gif.github.io/bloomdale-privacy-ai-governance/

References

Reviewed as of 15 November 2026.

- EU GDPR, Regulation (EU) 2016/679 (Articles 13–14, 21–22, 25, 35–36): https://eur-lex.europa.eu/eli/reg/2016/679/oj
- ICO, Examples of processing likely to result in high risk: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/
- ICO, When do we need to do a DPIA?: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/
- WP29 / EDPB Guidelines on DPIA (WP248 rev.01): https://ec.europa.eu/newsroom/article29/items/611236
- EDPB Guidelines 05/2021 on the interplay between Article 3 and Chapter V: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en
- ePrivacy Directive 2002/58/EC: https://eur-lex.europa.eu/eli/dir/2002/58/oj
- Data (Use and Access) Act 2025: https://www.legislation.gov.uk/ukpga/2025/18
- Connecticut data protection assessments, Conn. Gen. Stat. §42-522: https://codes.findlaw.com/ct/title-42-business-selling-trading-and-collection-practices/ct-gen-st-sect-42-522/
- California Privacy Protection Agency regulations (risk assessments, ADMT): https://cppa.ca.gov/regulations/
- Texas Data Privacy and Security Act, Tex. Bus. & Com. Code ch. 541: https://texas.public.law/statutes/tex._bus._&_com._code_section_541.002
- EU AI Act, Regulation (EU) 2024/1689: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- Regulation (EU) 2026/1744 amending the AI Act: https://eur-lex.europa.eu/eli/reg/2026/1744/oj
- NIST Privacy Framework: https://www.nist.gov/privacy-framework
- NIST AI Risk Management Framework: https://www.nist.gov/itl/ai-risk-management-framework

APPENDIX A | Assessment baseline reconciliation and publication controls

Version 1.2 | 15 November 2026 | Portfolio demonstration using fictional Meridian Digital Holdings and synthetic evidence. This appendix governs interpretation of the current case study and its companion risk register.

A1. Why the risk distribution changed

The earlier Phase 2 screening and Phase 3 draft register used an initial 8-risk distribution of four Critical and four High. During the consolidated v1.1 assessment, the team refined each scenario's likelihood, impact and scope against a defined AI-06 processing boundary: first-party product/content recommendations, excluding sensitive inferences, regulated HealthTech and Financial Services data, and consequential decisions. The current v1.2 baseline is one Critical, six High and one Moderate. This is an illustrative reassessment, not evidence that risks were mitigated or controls passed. The prior distribution is superseded for publication; it remains documented here as screening history.

The current baseline uses the eight risk-specific L × I scores in section 5. The companion workbook reproduces those scores and includes the preliminary distribution solely in a change log. No validated residual score exists. Every control test remains pending.

A2. Priority and release-gate clarification

Risk-action priorities (six P0, two P1) are distinct from control priorities (eight P0, two P1). R04 and R07 are P1 for tracking, but their mandatory pre-release protections are covered by P0 controls; any unfulfilled legal requirement or unacceptable risk is a release blocker regardless of priority. The production decision remains HOLD, with zero verified control evidence, zero completed risk actions, and zero validated residual scores.

A3. Regulatory applicability and dates: checked 15 November 2026

California CCPA risk assessments and ADMT

The CPPA regulations took effect 1 January 2026. Risk assessment compliance began 1 January 2026 for covered processing; ADMT Article 11 duties for significant decisions begin 1 January 2027. This first-party recommender is screened as outside the significant-decision ADMT trigger on stated facts, but risk assessment triggers require a separate documented determination.

Primary reference: https://cppa.ca.gov/announcements/2025/20250923.html

Colorado SB 26-189

The replacement automated decision-making law is scheduled to take effect 1 January 2027 and targets consequential decisions. This product/content recommender is outside that defined use on stated facts. Rulemaking and litigation/enforcement status should be rechecked before any real deployment.

Primary reference: https://leg.colorado.gov/bills/sb26-189

EU AI Act

Regulation (EU) 2026/1744 amended the AI Act in July 2026, including phased high-risk obligations. The defined recommendation-only use is not classified as Annex III high-risk; any change to employment, credit, education or other consequential use requires reassessment.

Primary reference: https://eur-lex.europa.eu/eli/reg/2026/1744/oj

GDPR and UK GDPR

GDPR Article 35 DPIA conclusion is scenario-specific and based on scale, systematic profiling and likely high-risk criteria, not an assertion that ordinary product recommendations automatically trigger Article 35(3)(a). Consent, legitimate interests, cookies, objection rights and cross-border processing require distinct jurisdictional analysis.

Primary reference: https://eur-lex.europa.eu/eli/reg/2016/679/oj

A4. Publication quality gates

The package contains the current consolidated case study and executive dashboard, approved enterprise SOP and two Privacy by Design checklists, a synchronized v1.2 risk register, and a README. BDC-PRIV-001 v2.2 is an existing cross-reference, not a second copy of the enterprise assessment. All materials are simulated and are not evidence of a live OneTrust tenant, completed tests or real regulatory advice.