Enterprise DSAR Management & Consumer Rights Operations

BDC-OPS-001 | Consolidated case study v3.0 | 12 November 2026

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

Published by BloomDale Capital LLC • Fictional enterprise: Meridian Digital Holdings • Data snapshot: 11 November 2026

SIMULATION DISCLOSURE All organizations, systems, people, request records and metrics are fictional. Interface images are original illustrations, not OneTrust screenshots. This is a portfolio demonstration, not an employer implementation or legal advice. Legal references were reviewed as of 12 November 2026. OneTrust is a trademark of its owner; no affiliation, sponsorship or endorsement is implied.

1. Executive overview

Meridian Digital Holdings (MDH) is a fictional group with Digital Platforms, Digital Learning, Financial Services and Healthcare Technology businesses. Its privacy requests arrived through scattered channels, with inconsistent evidence and no shared view of deadlines. This case study designs a centralized consumer rights operation: one procedure, one register, law-specific deadline rules and management reporting, with OneTrust Privacy Rights Automation as the proposed case-management platform.

The synthetic register of 12 requests shows why the reporting design matters. Every closed request met its statutory deadline, yet only three of eight met Meridian's own internal target, and two open requests were already past their legal deadline on the snapshot date.

Measure (as of 11 November 2026)	Result	What it shows
Requests in the register	12 (8 closed, 4 open)	Synthetic data across six regimes
Closed within statutory deadline	8 of 8 (100%)	Covers closed cases only
Closed within internal target	3 of 8 (37.5%)	Operations run close to the legal limit
Open past statutory deadline	2 (MDH-26008, MDH-26010)	Reported separately from the closed-case rate
Average days to close	24.4 (30.0 excluding opt-outs)	Fast opt-outs flatter the overall average

The main design decision follows from this: closed-case timeliness, open-case deadline exposure and internal-target performance are always reported side by side, so a 100% figure cannot hide overdue work.

2. Enterprise context and scope

Meridian is the same fictional enterprise assessed in case study BDC-PRIV-001, and this study follows its applicability screening. The regimes in scope are the CCPA/CPRA (California), the Connecticut Data Privacy Act (in scope since 1 July 2026), the Texas Data Privacy and Security Act, the EU GDPR and the UK GDPR. Meridian HealthTech handles health requests as a HIPAA business associate. Residents of other states are

served under a voluntary baseline policy with a 45-day internal standard; those states are monitored and added to the deadline rules if Meridian crosses their thresholds.

Business unit	Typical requests	Routing rule
Digital Platforms	Access, erasure, opt-out of sale/sharing and targeted advertising	Consumer privacy law of the requester's jurisdiction; EU and UK users under GDPR
Digital Learning	Access, deletion, portability	As above; EU and UK learners under GDPR
Financial Services	Access, deletion, correction	GLBA-covered account data is exempt at data level under the CCPA and CTDPA; the unit is entity-exempt under the TDPSA
Healthcare Technology	Access to and amendment of PHI	Business associate: forward to the covered entity under the BAA and support fulfillment; the covered entity decides

3. Governance and control ownership

Control area	Accountable / responsible	Evidence
Intake and case ownership	Privacy Operations Lead / analyst	Receipt timestamp, intake channel, case ID
Applicable law and exceptions	Legal accountable; Privacy Operations responsible	Jurisdiction decision, denial or retention rationale
Identity and secure delivery	Privacy Operations; Security consulted	Verification outcome, secure response method
Discovery and fulfillment	IT, business system owners and processors	Assigned tasks, completion attestations
Business associate requests	Health Privacy; covered entity decides	Forwarding record, BAA timeline, fulfillment support
Monitoring and escalation	Privacy Operations Lead	Aging report, deadline alerts, escalation record

4. Standard operating procedure

1. **Intake and register.** Accept requests through the web form, privacy inbox, support escalation and authorized agents. Record the original receipt date (the clock starts that day, even on a weekend), request type, business unit, channel and case ID. Check for duplicates and send any required acknowledgment (CCPA: within 10 business days).
2. **Classify and set the deadline.** Identify the applicable law, Meridian's role (controller, business or business associate), exemptions and the right requested. Record the statutory due date, the internal target and the last date to send an extension notice. Calendar-month and calendar-day rules are calculated separately.
3. **Verify where appropriate.** Use existing account authentication where possible and avoid collecting new government ID. Do not verify opt-out requests. Follow up by day 10. An unverified request then goes to a

decision gate (day 35 for 45-day regimes; day 20 for GDPR, UK GDPR and HIPAA): deny as unverifiable, or send an extension notice where the law allows one.

4. **Discover and assign.** Use the data inventory and vendor register to assign tasks to CRM, LMS, marketing, payment, cloud and processor owners, each with a due date and an evidence requirement.
5. **Fulfill and review exceptions.** Process access, correction, deletion, portability and opt-out actions. Legal reviews retention duties, legal holds, security exceptions, third-party data and partial denials. Suppression is tracked separately from deletion.
6. **Validate and respond.** QA reconciles task outcomes, checks redaction and secure delivery, confirms suppression reached downstream systems and approves the response, including appeal or complaint information where the law requires it.
7. **Close and report.** Close only after QA sign-off. Retain minimum evidence under the retention schedule and feed the case into SLA, aging, exception and vendor-performance reporting.

5. Lifecycle and decision points

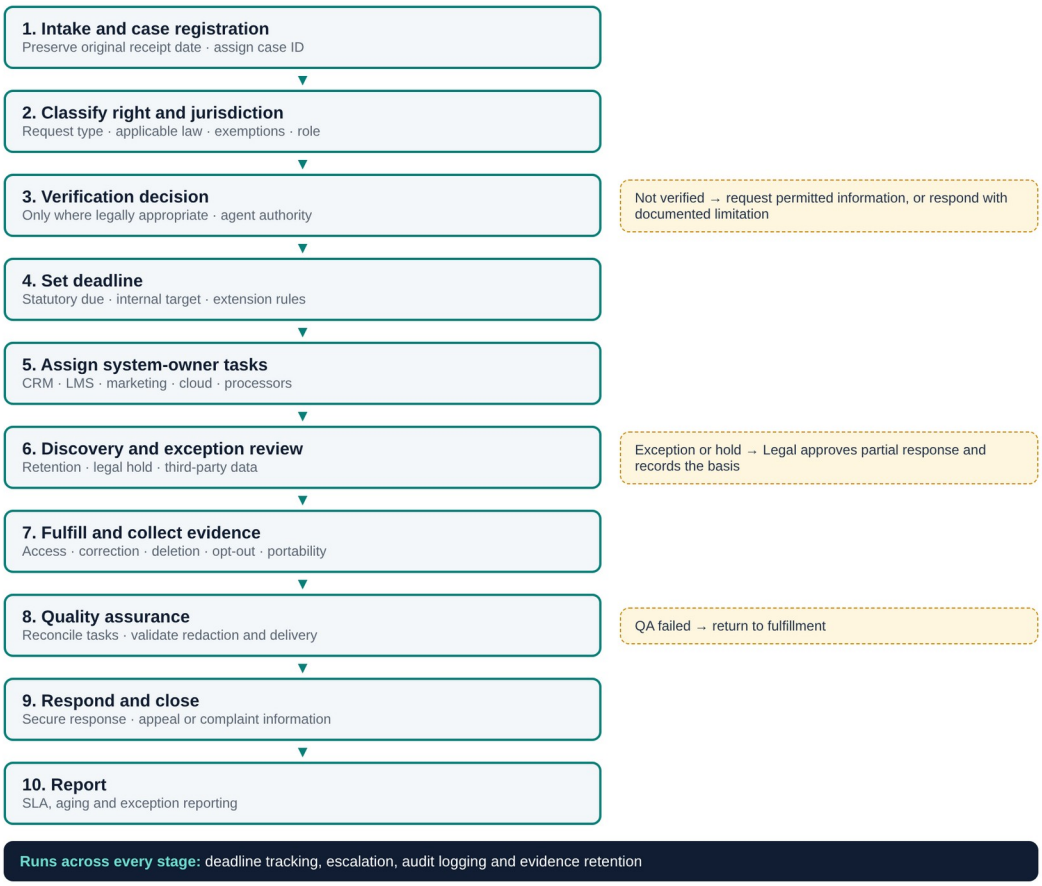


Figure 1. DSAR lifecycle with decision branches. Original illustration.

Decision point	Required response
Verification required?	Apply proportionate verification only where lawful; never for opt-out requests.
Verified?	Request additional information as permitted; record the follow-up and its effect on the deadline.
Request within scope?	Identify the controlling law and exemptions; Legal approves any denial or partial response.
Retention or legal hold?	Document the preservation basis, fulfill the remainder and consider restriction or suppression.
QA passed?	Reassign incomplete tasks; do not close without evidence and an approved response.

6. Regulatory rights and deadline matrix

Response rules for the regimes in scope, reviewed as of 12 November 2026. Deadlines run from receipt and assume no extension; they drive the register's Statutory Due field.

Regime	Response deadline	Extension	Verification and special rules	Appeal or redress
EU GDPR	One calendar month from receipt (Art. 12(3))	Up to two further months if complex or numerous; notify within the first month	Extra information only where there is reasonable doubt about identity (Art. 12(6))	Complaint to a supervisory authority; judicial remedy
UK GDPR	One calendar month; if that date is a weekend or bank holiday, the next working day (ICO)	As EU GDPR	The month runs from the latest of receipt, receipt of identity information requested under Art. 12(6), or any fee; it pauses while awaiting clarification reasonably required (Art. 12A, in force 5 February 2026)	Complaint to Meridian under its complaints procedure (required since 19 June 2026; acknowledge within 30 days); complaint to the ICO; judicial remedy
CCPA/CPRA	45 calendar days for know, delete and correct, from receipt regardless of verification time; confirm receipt within 10 business days	One 45-day extension with notice and reason inside the first 45 days	Opt-out of sale/sharing and limit-use requests: no verification; act within 15 business days	No statutory appeal
Connecticut (CTDPA)	45 days	One 45-day extension when reasonably necessary, with notice inside the first 45 days	Honor opt-out preference signals; authenticate other requests with commercially reasonable efforts	Appeal decided within 60 days; if denied, provide the Attorney General complaint route

Regime	Response deadline	Extension	Verification and special rules	Appeal or redress
Texas (TDPSA)	45 days	One 45-day extension when reasonably necessary, with notice and reason inside the first 45 days	Authenticate requests with commercially reasonable methods; honor universal opt-out signals	Appeal decided within 60 days; if denied, provide the Attorney General complaint route
HIPAA (Meridian as business associate)	Covered entity acts on access within 30 days and amendment within 60 days (45 CFR 164.524, 164.526)	One 30-day extension each, with written notice	Meridian forwards the request within the BAA timeframe and supports fulfillment	Covered entity handles denials; complaints to HHS OCR
GLBA / Regulation P	No access, deletion or correction right	Not applicable	Privacy notices; opt-out of certain sharing with nonaffiliated third parties	GLBA-covered data exempt from state requests at data level (CCPA, CTDPA) or entity level (TDPSA)

7. OneTrust operating model

Each lifecycle stage maps to a proposed use of OneTrust Privacy Rights Automation and to the register field that evidences it.

Lifecycle stage	Proposed OneTrust use	Register field and evidence	Owner
Intake and registration	Request intake form and case record; manual case creation for email and phone	Columns A to E; receipt timestamp	Privacy Operations
Verification	Verification as a workflow task, skipped for opt-outs	Column H; verification log	Privacy Operations
Classification and deadline	Request type, jurisdiction and deadline rules	Columns C, D, F and G	Privacy Operations; Legal
Fulfillment	Subtasks for system owners and processors; integrations where licensed	Columns J and O; task evidence	System owners
Exceptions	Legal approval step with recorded rationale	Column K	Privacy Legal
Response and closure	Approved templates, secure delivery, QA sign-off	Columns L to N and Q	Privacy Operations
Reporting	Volume, aging and SLA reports reconciled to the register	Dashboard workbook	Privacy Operations Lead

The table describes a proposed design. Stage names are not verified OneTrust menu names or default features, and no live OneTrust tenant was configured. Product capabilities should be confirmed in OneTrust's documentation (see References).

8. Illustrative interfaces

Figures 2 to 5 are original illustrations built from the synthetic register to show how the operating model would look in daily use. They are not OneTrust screenshots and do not reproduce OneTrust's interface.

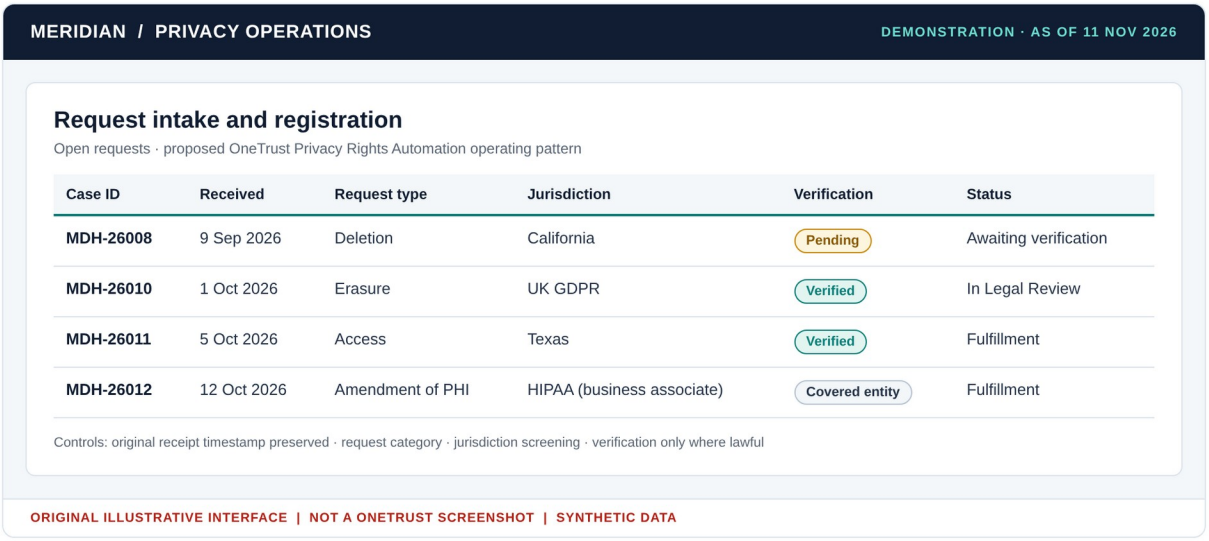


Figure 2. Intake queue for the four open requests, with conditional verification; the HIPAA request has been forwarded to the covered entity.

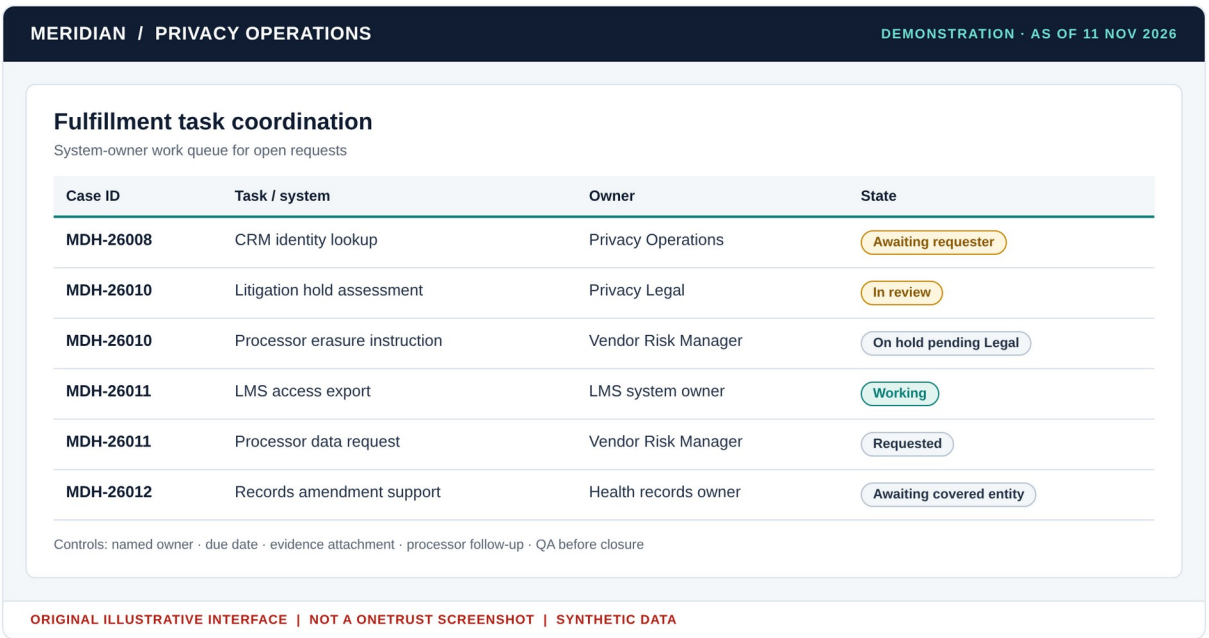


Figure 3. Task coordination across Privacy Operations, Legal, system owners and processors.

MERIDIAN / PRIVACY OPERATIONS — DEMONSTRATION · AS OF 11 NOV 2026

Deadline and escalation monitoring

Proposed case-management rules, not verified OneTrust defaults

Case ID	Statutory due	Internal target	Days to statutory due	Risk	Action
MDH-26008	24 Oct 2026	9 Oct 2026	−18	Overdue	Escalate to Privacy Legal
MDH-26010	2 Nov 2026	21 Oct 2026	−9	Overdue	Legal decision on exemption
MDH-26011	19 Nov 2026	4 Nov 2026	8	Past internal target	Expedite processor tasks
MDH-26012	11 Dec 2026	11 Nov 2026	30	Internal target today	Confirm covered-entity decision

Reminders at 15, 7 and 3 days before the internal target · statutory due assumes no extension · HIPAA date belongs to the covered entity

ORIGINAL ILLUSTRATIVE INTERFACE | NOT A ONETRUST SCREENSHOT | SYNTHETIC DATA

Figure 4. Deadline monitoring as of 11 November 2026: two overdue cases, one past its internal target and one at its internal target today.

MERIDIAN / PRIVACY OPERATIONS — DEMONSTRATION · AS OF 11 NOV 2026

Privacy operations reporting

Metrics recalculated from the synthetic case register

TOTAL REQUESTS	CLOSED ON TIME	OPEN PAST DUE	AVG CLOSE DAYS
12	100%	2	24.4
8 closed · 4 open	8 of 8, statutory deadline	MDH-26008, MDH-26010	30.0 excluding opt-outs

WITHIN INTERNAL TARGET	OPEN PAST INTERNAL TARGET	DUE IN NEXT 15 DAYS	APPEALS FILED
37.5%	3	1	0
3 of 8 closed cases	Includes both overdue cases	MDH-26011, due 19 Nov	2 cases eligible

Closed-case on-time rate does not establish overall program compliance; overdue open cases are reported separately.

ORIGINAL ILLUSTRATIVE INTERFACE | NOT A ONETRUST SCREENSHOT | SYNTHETIC DATA

Figure 5. Management reporting recalculated from the register.

9. Case register and dashboard results

All figures are recalculated from the 12 rows of the synthetic case register as of 11 November 2026 and match the companion dashboard workbook; the appeals tile in Figure 5 is counted from the register's Appeal column.

Metric	Definition	Result
Closed on time (statutory)	Closed cases with closure date on or before Statutory Due, divided by closed cases	8 of 8 (100%)
Open past statutory due	Open cases whose Statutory Due is before the snapshot date	2
Closed within internal target	Closed cases with closure date on or before Internal Target, divided by closed cases	3 of 8 (37.5%)
Open past internal target	Open cases whose Internal Target is before the snapshot date	3
Average days to close	Calendar days from receipt to closure, closed cases	24.4
Average days to close, excluding opt-outs	As above, rights requests only	30.0
Due in next 15 days	Open cases due within 15 days of the snapshot date	1 (MDH-26011)

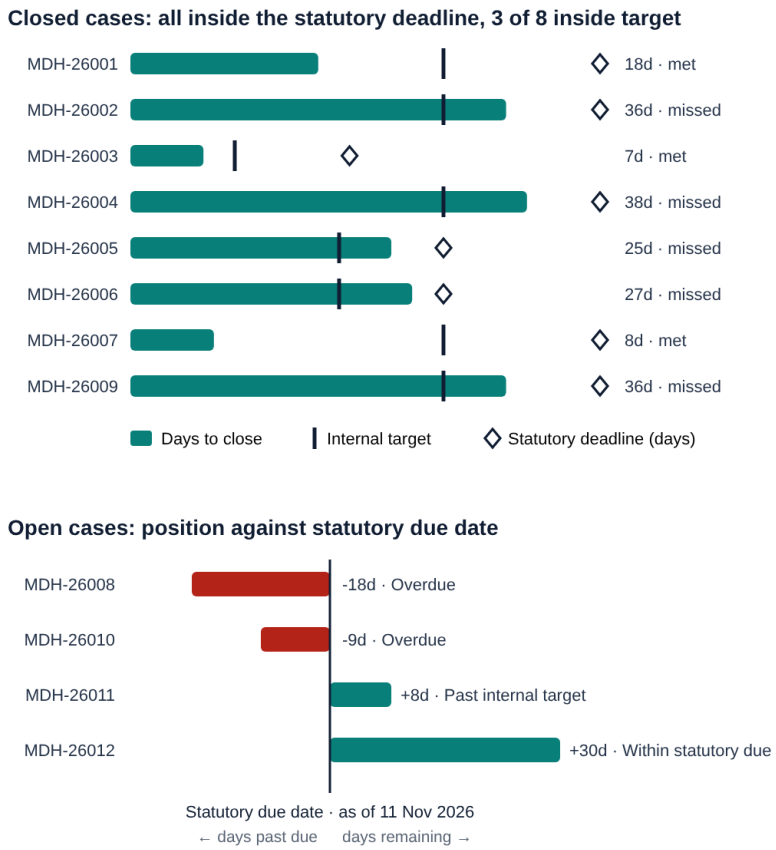


Figure 6. Closed-case cycle time against targets (top) and open-case position against the statutory due date (bottom).

- All eight closed requests met the legal deadline, but five missed the internal target: MDH-26002, 26004, 26005, 26006 and 26009. Each involved Legal review, several systems or a third party.
- The overall average of 24.4 days rises to 30.0 days once two opt-outs, closed in 7 and 8 days, are excluded; 30.0 is the more representative measure of rights-request handling.
- Two open requests are past their legal deadline. A closed-case rate of 100% must never be presented as overall compliance.

10. Worked case: MDH-26002

A Texas learner asks Digital Learning to delete their data. The case shows a lawful partial deletion that met the legal deadline but missed the internal target.

Date (2026)	Day	Step
5 August	0	Request received through the privacy web form; case created. Statutory due 19 September (45 days); internal target 4 September.
6 August	1	Identity verified through existing learner-account authentication.
7 August	2	Deletion tasks assigned to LMS, CRM, marketing and billing owners.
21 August	16	LMS, CRM and marketing confirm deletion; billing flags invoices needed for tax records.
1 September	27	Legal approves retaining invoice records for the tax retention period; all other data deleted.
10 September	36	QA sign-off. The response explains what was deleted, what was kept and why, and how to appeal. Case closed.

Outcome: closed nine days before the statutory deadline but six days after the internal target, because the Legal exception review took 11 days.

Improvement: pre-approved retention rules for standard record types (tax, fraud, legal hold), so Legal reviews only new kinds of exception.

11. Overdue and at-risk cases

MDH-26008: California deletion, Financial Services (due 24 October 2026, 18 days overdue)

Status: verification request sent; no reply.

Why it is late: the CCPA's 45-day period runs from receipt regardless of verification time. No extension notice was sent, and no rule forced a decision on an unverified request.

Action now: respond that identity could not be verified and the deletion request is denied (11 CCR 7022(a)), explaining the basis, including that GLBA-covered account data is exempt in any case (7022(f)). If Meridian sells or shares this person's data and they have not opted out, ask whether they want to opt out of sale/sharing and include the opt-out notice or a link to it (7022(g)); an opt-out needs no verification. Record the late response.

Control fix: verification follow-up on day 10 and a decision gate on day 35 for 45-day regimes (verify, deny as unverifiable, or extend with notice).

MDH-26010: UK GDPR erasure, Digital Platforms (due 2 November 2026, 9 days overdue)

Status: litigation hold under Legal review.

Why it is late: Legal review had no time limit and no extension notice went out within the first month. An internal review does not pause the clock; under Article 12A only a request for information reasonably required does.

Action now: decide whether the Article 17(3)(e) exemption covers data needed for legal claims; erase or restrict the rest; instruct processors; tell the person what was and was not erased, why, and how to complain to Meridian and to the ICO.

Control fix: a 10-day limit on Legal decisions and an extension decision by day 20 of the month.

MDH-26011: Texas access, Digital Learning (due 19 November 2026, past internal target)

Status: processor tasks outstanding.

Action now: escalate through the Vendor Risk Manager; if processors cannot deliver in time, send the TDPSA extension notice, stating the reason, no later than 19 November.

Control fix: contractual processor response times, tracked as a vendor KPI.

12. Controls and assurance

Risk	Control	Test evidence
Missed legal deadline	Deadline rules by regime, reminders, day-35 decision gate, escalation	Deadline sample test; overdue exception review
Unauthorized disclosure	Proportionate verification and secure delivery	Access controls and delivery validation
Incomplete deletion	Inventory-driven task assignment and reconciliation	System-owner evidence and QA sign-off
Unlawful deletion	Legal retention and legal-hold checkpoint	Approved exception rationale
Processor gap	Processor task ownership and contractual response times	Vendor attestation and exception tracking
Business associate routing error	BAA-based routing rule; Health Privacy review	Sample of forwarding records
Misleading reporting	Closed-case, open-case and internal-target metrics reported together	Reconciliation of dashboard to register

13. Limitations

- All organizations, records and metrics are synthetic. Dates, owners and outcomes illustrate the operating model and are not performance evidence.
- The regulatory matrix is a screening reference as of 12 November 2026, not legal advice. Weekend roll-forward is applied to EU and UK GDPR deadlines; public holidays are not modeled, and no register deadline falls on one. No extensions are applied in the register.
- OneTrust is referenced as an example platform. The study does not represent a configured tenant, an endorsement or an affiliation.

- HIPAA handling assumes Meridian HealthTech acts as a business associate, consistent with BDC-PRIV-001, and conservatively runs the covered entity's deadline from Meridian's receipt.

14. Companion files

- **BDC-OPS-001_Synthetic_DSAR_Case_Register_v1.1.xlsx**: master case register with field guide and KPI snapshot.
- **BDC-OPS-001_DSAR_SLA_Dashboard_v1.1.xlsx**: executive dashboard with charts; holds a copy of the register for its formulas.
- **BDC-PRIV-001**: the enterprise privacy assessment that sets Meridian's profile and applicability screening.

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 12 November 2026.

- EU GDPR, Regulation (EU) 2016/679: https://eur-lex.europa.eu/eli/reg/2016/679/oj
- ICO, Right of access: responding to a request: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/what-should-we-consider-when-responding-to-a-request/
- Data (Use and Access) Act 2025: https://www.legislation.gov.uk/ukpga/2025/18
- CCPA regulations, 11 CCR §7021 (response timelines): https://www.law.cornell.edu/regulations/california/11-CCR-7021
- CCPA regulations, 11 CCR §7022 (requests to delete): https://www.law.cornell.edu/regulations/california/11-CCR-7022
- California Privacy Protection Agency regulations: https://cppa.ca.gov/regulations/
- Connecticut Attorney General (CTDPA): https://portal.ct.gov/ag
- Texas Data Privacy and Security Act, Tex. Bus. & Com. Code §541.052 (responses and extensions): https://texas.public.law/statutes/tex._bus._&_com._code_section_541.052
- HIPAA Privacy Rule, 45 CFR Parts 160 and 164: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C
- CFPB Regulation P, 12 CFR Part 1016: https://www.ecfr.gov/current/title-12/chapter-X/part-1016
- OneTrust Privacy Rights Automation (product page): https://www.onetrust.com/products/privacy-rights-automation/
- OneTrust documentation: https://docs.onetrust.com/