UNLOCKING DATA THROUGH PRIVACY GOVERNANCE:

HOW TO ‘SAY YES' WHILE MINIMIZING RISK

SPEAKERS

JOANNE CHARLES

Gilead Sciences

Joanne.Charles@gilead.com

ELLIOT GOLDING

McDermott Will & Schulte

Egolding@mwe.com

AMY PAPSUN

Headway

Amy.papsun@findheadway.com

SESSION OVERVIEW

AGENDA

TODAY'S SESSION: Three areas of focus to help your team see around corners, identify risk proactively, and build durable governance.

GOAL: Equip teams with a clear view of the US privacy landscape, a governance framework, and a practical decision-making process

01

Update on US Privacy Landscape

Current state of federal and state privacy legislation, sector-specific regulations (HIPAA, CMIA), and emerging enforcement trends that affect data strategy.

02

Data Governance Strategy & Framework

An enterprise framework for managing data provenance, minimization, retention, and consent — structured to align legal obligations with operational realities.

03

Business Decision-Making Process

A structured step-by-step process to help teams see around corners, proactively identify risks, and reach confident, defensible 'yes' or 'no' decisions on data use cases.

US PRIVACY LANDSCAPE

US REGULATION IS INCREASING

U.S. Laws and Regulation

- State Privacy Laws (new comprehensive + sector-specific (health, financial, insurance, etc.))
- Federal Sectoral Laws (HIPAA, GLBA, Part 2, etc.)
- UDAP Laws (FTC Act, state equivalents, etc.)
- Marketing Rules (TCPA, CAN-SPAM, etc.)
- Other Laws Governing Data (Common Rule, Information Blocking, Interoperability Regs
- Outdated laws applied to new technologies (CIPA/Wiretap laws, Video Privacy Protection Act)

Guidance

- Cookies/Online Activity Guidance: FTC (link); OCR (link); NY AG (link)
- HHS Health App, Cloud Computing, etc.

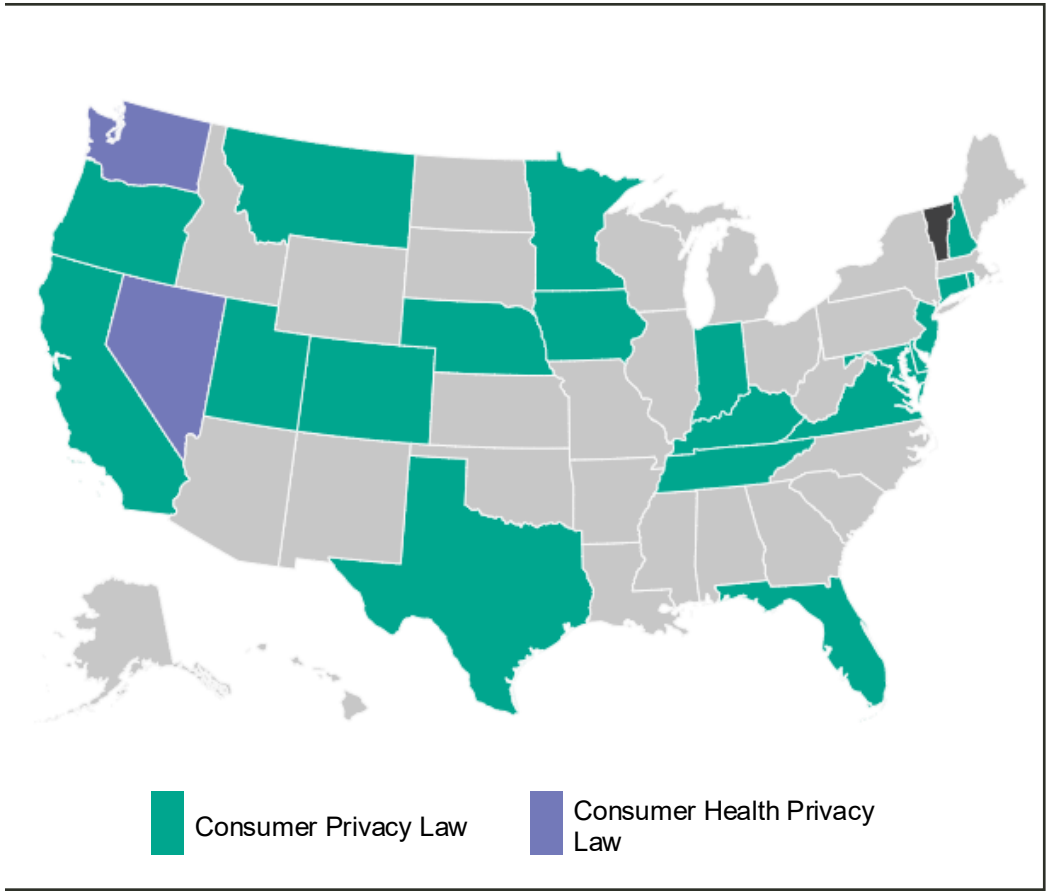
NUMBER OF STATE PRIVACY LAWS IS INCREASING

22

States have enacted consumer privacy laws

20 CURRENTLY IN EFFECT (+ OK + AL SOON):

- California
- Virginia
- Colorado
- Connecticut
- Utah
- Texas
- Florida
- Oregon
- Minnesota
- Montana
- Iowa
- Delaware
- Nebraska
- New Hampshire
- New Jersey
- Tennessee
- Maryland
- Kentucky
- Rhode Island
- Indiana



https://www.mcdermottlaw.com/resource/global-privacy-cybersecurity-resource-center/#map

GOVERNANCE RISKS

OVER-RETENTION: WHAT HAPPENS WHEN WE KEEP DATA TOO LONG

REGULATORY REQUIREMENT: Companies must not keep personal data longer than necessary for its original purpose. Data must be deleted or anonymized on schedule.

COMPLIANCE ACTIONS: Follow the retention schedule • Delete data you no longer need • Collect only the data you actually use (data minimization)

KEY RISK: OVER-RETENTION

WHAT CAN GO WRONG

SECURITY RISK

Keeping extra data makes breaches worse

The more data we store, the more attackers can steal. Most ransomware attacks now copy data before encrypting it.

A smaller data footprint means less exposure if something goes wrong.

ENFORCEMENT RISK

Regulators can fine you for keeping data too long

Privacy regulators are actively targeting companies that retain data beyond its legal purpose, especially when over-retention makes a breach worse.

Applies under: CCPA, GDPR, HIPAA, and UDAP laws.

LITIGATION & COST RISK

Lawsuits and operating costs both rise

Plaintiffs are suing over excess data retention. Class actions are increasing under CCPA. Storage, discovery, and privacy request costs rise with data volume.

Excess data means excess liability and cost.

Applicable Regulations: CCPA/CPRA • GDPR • HIPAA • 21 CFR Part 11 • FTC Act Section 5 (UDAP) • EU AI Act • Colorado AI Act • State UDAP

ENFORCEMENT: EXAMPLES

CA AG: **Blackbaud**

$675 million settlement and corrective action plan.

"Blackbaud stored data . . . for years longer than necessary . . . . Had Blackbaud implemented data minimization principles or appropriate retention policies, it could have mitigated the threat actor's exfiltration of data."

NY DFS: **Eyemed**

$4.5 million settlement.

"Moreover, because EyeMed failed to implement a sufficient data minimization strategy and disposal process for the Mailbox, the compromised shared Mailbox contained old data that was accessible to the threat actor. Proper disposal processes minimize the amount of NPI accessible to an unauthorized third party during a Cyber Event."

FTC: **InMarket Media**

20-year order to maintain retention schedule and delete historical data.

Data was allegedly kept "far longer than is necessary to accomplish InMarket's stated purpose … InMarket's comprehensive collection and long-term retention of location data subjects consumers to a likelihood of substantial injury."

GOVERNANCE RISK: UNAUTHORIZED SECONDARY USE OF DATA

REGULATORY CONTEXT: Data collected for one purpose may not be reused without compatible notice and consent. CCPA/CPRA purpose limitation and FTC unfair/deceptive practices doctrine both apply.

COMPLIANCE ACTIONS: Enforce purpose binding at dataset/model level • Review AI training data sourcing • Update notices before reuse

KEY RISK: PURPOSE CREEP & UNAUTHORIZED DATA REUSE

WHAT CAN GO WRONG

REGULATORY RISK

CCPA/CPRA purpose limitation and FTC enforcement

CCPA/CPRA bars secondary use without compatible purpose or new consent. FTC treats undisclosed data reuse as an unfair/deceptive practice. Increasing regulatory scrutiny of AI model training using customer or patient data. Example: Using patient support data to train commercial targeting models.

No enforceable purpose binding = regulatory and litigation exposure.

AI TRAINING & ANALYTICS RISK

AI and analytics reuse of original-purpose data

Regulators are scrutinizing whether AI training on customer data constitutes a new, undisclosed purpose. Governance gap: no enforceable purpose-binding mechanism at the dataset or model level. Without it, analytics enrichment and model training from original-purpose data creates compounding exposure.

AI training from operational data requires fresh legal analysis before proceeding.

Applicable Regulations: CCPA/CPRA • FTC Act Section 5 (UDAP) • HIPAA • EU AI Act • Colorado AI Act • State Consumer Protection Acts

HISTORICAL ENFORCEMENT

AGENCY	FACT	CAUSE OF ACTION	STATUS
FTC	Avast (antivirus/software provider) sold identifiable **browsing data** without notice/consent	**UDAP**	Settled for $16.5 million + 20-year CAP
FTC	Kochava (data broker) sued for selling sensitive data (including **geolocation**)	**UDAP**	Pending
CA AG	Food delivery company sold data to **marketing cooperatives** without notice under CCPA (notice and DNS) and CalOPPA (notice)	**CCPA & CalOPPA**	Settled for $375k + CAP
CA AG	Sephora (cosmetic retailer) failed to (i) **inform** consumers it sold data collected via its website and (ii) **honor opt-out requests**	**CCPA**	Settled for $1.2 million + regular compliance reports to the CA AG
FTC	X-Mode/Outlogic (data broker) sold raw location data with sensitive locations and failed to implement reasonable safeguards against downstream use of **precise location data**	**UDAP**	Banned from sharing or selling sensitive location data
FTC	Data aggregator failed to fully inform consumers and obtain consent before collecting and using **precise location data** for advertising and marketing	**UDAP**	Banned from selling or licensing precise geolocation data
FTC	BetterHelp (online counseling service) revealed data to **social media companies** for advertising purposes	**UDAP**	Settled for $7.8 million

GOVERNANCE RISK: WHAT HAPPENS WITH COOKIE DATA

REGULATORY CONTEXT: Cookies collecting personal data can trigger wiretap laws, UDAP, and privacy regulations. Adequate notice and consent are required to minimize risk.

COMPLIANCE ACTIONS: Provide adequate notice • Obtain affirmative consent • Implement cookie governance program

KEY RISK: COOKIE LITIGATION & ENFORCEMENT

WHAT CAN GO WRONG

LITIGATION RISK

Wiretap violations carry significant damages

Wiretap laws: up to **$10k/violation** (ECPA); states $1k-$5k. 30+ plaintiffs firms filing demand letters and litigation. Public settlements range **$2M-$18M**. Recent jury verdicts going against defendants.

Even good-faith cookie programs face class action exposure.

ENFORCEMENT RISK

Regulators impose sweeping remedies on violators

State regulators targeting health companies on non-exempt data. FTC 20-year consent decrees require: affirmative consent, ban on data selling, algorithm deletion, comprehensive privacy programs, third-party assessments, and monetary disgorgement.

Regulators are increasingly targeting health sector cookie practices.

Applicable Regulations: CCPA/CPRA • GDPR • HIPAA • FTC Act Section 5 (UDAP) • ECPA • State Wiretap Laws • State Consumer Protection Acts

LESSONS FROM RECENT ENFORCEMENT (PUBLIC/NON-PUBLIC)

Non-Verifiable vs. Verifiable Requests	• Verification prohibitions
	  • Too much info requested
	  • No webform for logged-in users
	• Authorized Agents

Opt-Out Requests	• Friction (where and how choice is presented) • Single click / minimizing steps • But: Cookie-based vs. non-Cookie-based • Opt-out known users across devices/platforms/services • Immediate effect and flow down • Dark patterns + symmetry in choice
SPI	• Broad view of "health inferences" • Opt-in needed for secondary purposes (*Healthline*)
DSR Responses	• Timeliness • Statistics (Grant vs. Deny) • Particularized Reasons for Denial
Contracts	• C2C contracts

RECENT STATE LAW EXAMPLES

Agency	Target Company	Key Allegations	Penalties
CA AG	Healthline	• Failed to honor consent choices (by misconfiguring cookie consent tool). • Shared health-related article titles with third parties, which CA AG alleged violated the CCPA's "purpose limitation" because it was an unexpected use of "sensitive personal information" (SPI). • Note: Calls into question the ability to use trackers for health marketing at all. • Failed to offer consumers a right to limit SPI processing. • Failed to include required terms in contracts with advertising companies.	• $1.55 million settlement • Data disgorgement • Prohibition of certain data "sales" altogether
CalPrivacy	Honda	• Required more steps to opt out of sale/sharing than to opt back in. • Requested excessive information to process data subject rights requests. • Required verification for authorized agent requests to opt out of sale/sharing. • Failed to execute required contracts with advertising technology partners.	• $632,500 fine
CalPrivacy	Todd Snyder	• Failed to properly configure privacy portal and cookie banner and continued to sell personal information via tracking technologies after consumers requested to opt out. • Required consumers to submit more information than necessary to process privacy requests. • Required consumers to verify their identity before they could opt out of the sale or sharing of their personal information.	• $345,178 fine
CalPrivacy	Tractor Supply	• Failed to: (i) inform consumers about how to opt out of sale/sharing through tracking technologies; (ii) honor browser-based opt-out through webform; and (iii) honor GPC • Failed to execute required contracts with advertising technology partners. • Failed to inform consumers and job applicants of their CCPA rights and how to exercise them; failed to update consumer privacy notice annually.	• $1.35 million fine • Onerous remedial measures (e.g., quarterly website scans, inventory, updating/distributing notices, etc.) • Annual compliance certification

RECENT STATE LAW EXAMPLES (CONT)

Agency	Target Company	Key Allegations	Penalties

CalPrivacy	Disney	• Failed to provide single method for logged-in users to opt out of all sales across all services and all devices by, e.g.:
		  • Applying opt-out requests to a single device or single streaming service
		  • Making opt-out processes overly complex and difficult to use
		  • Treating GPC signals as device specific
			$2.75M fine + remedial measures

CalPrivacy	PlayOn Sports	• Failed to provide method to opt out of sale/sharing through tracking technologies. • Failed to honor GPC • Notices didn't include all information required by CCPA • Forced customers to "agree" to cookie deployment (particularly because data included minors' data)	Settled for $1.1 million + remedial measures
TX AG	Samsung, LG, Sony, Hisense, TCL	• Failed to adequately disclose use of Automated Content Recognition (ACR) technology • Failed to obtain consent from users for ACR • Disclosures that were made were buried, unclear, or misleading • *Hisense and TCL only*: Failed to disclose that company is required to transfer personal data to PRC under Chinese law	• Samsung: Settled with remedial measures • Hisense: TX obtained TRO, case proceeding • LG: Case proceeding • TCL: Case proceeding • Sony: Case proceeding

GOVERNANCE RISK: THIRD-PARTY & VENDOR DATA MISUSE

REGULATORY CONTEXT: Vendors using enterprise data for their own purposes — including model training or analytics enrichment — triggers CCPA service provider vs. third-party distinctions and creates contractual and regulatory liability.

COMPLIANCE ACTIONS: Add AI/data-use restrictions to all vendor contracts • Require audit rights • Classify vendors as service providers under CCPA

KEY RISK: VENDOR AI DATA EXPLOITATION & PRIVILEGE EROSION

WHAT CAN GO WRONG

CONTRACTUAL & REGULATORY RISK

Vendor contracts that lack AI data-use limits create liability

CCPA distinguishes service providers (who may not use data for their own purposes) from third parties (who may). Contracts that fail to establish service-provider status expose enterprise data to vendor reuse. Absence of audit rights means violations may go undetected. Example: SaaS AI tool training on internal documents or communications.

Standard vendor contracts rarely address AI data use — a critical gap.

PRIVILEGE & CONFIDENTIALITY RISK

Sensitive internal data ingested into vendor AI systems

When attorney-client privileged communications, trade secrets, or confidential strategy documents are processed by vendor AI tools, they may be incorporated into model weights or training logs, eroding privilege and exposing confidential information. Many SaaS AI platforms retain inputs for model improvement without explicit opt-out.

Privilege waiver risk is irreversible once sensitive data enters vendor AI systems.

Applicable Regulations: CCPA/CPRA • DTSA • FTC Act Section 5 • HIPAA • State Trade Secret Laws • Contract Law

DATA GOVERNANCE & STRATEGY

DATA GOVERNANCE

AT ITS CORE

The foundational elements that every data governance program must address — and that legal analysis must account for in a holistic process.

CORE FRAMEWORK ELEMENTS

- Core Values & Principles
- Roles & Responsibilities
- Rules of Engagement
- Processes
- Data Lifecycle Management
- Privacy by Design & Data Provenance
- Use & Disclosure Approval Process
- Third-Party Management
- Ongoing Feedback Loop

DATA GOVERNANCE

GOALS

NORTH STAR: Five strategic outcomes that define success for the data governance program — guiding every framework, process, and decision.

TOGETHER THESE GOALS: Maximize data rights and flexibility while keeping risk, time-to-decision, and regulatory exposure to a minimum

KEY MEASURE: Progress on all five goals is tracked and reported through the governance program's ongoing feedback loop

Unified Data Strategy

Develop and implement unified data strategy, governance, and decision-making processes across the organization

Maximize Data Rights & Flexibility

Preserve maximum rights and flexibility over data assets to enable current and future product opportunities

Reduce Time to Decision

Streamline the process for making product decisions on data use cases. Faster answers, fewer blockers

Enhance Transparency

Build a clear, documented, and explainable decision-making process that stakeholders at all levels can follow

Minimize Risk

Reduce regulatory, litigation, and reputational exposure by embedding risk assessment into every data decision

GETTING TO “YES”

Key Considerations to Guide Decision-Making

Four tensions that shape every privacy and data governance analysis.

Compliance Cost & Timing

Privacy law compliance carries real costs: legal review, technical controls, consent infrastructure, and vendor diligence. Timing matters, too. Retrofitting compliance after a product launches is far more expensive than building it in. Counsel should flag where compliance investment is required early and where timing creates legal exposure.

Data Flexibility

Businesses often want maximum freedom to use data for analytics, product improvement, and monetization. Privacy law constrains that flexibility through purpose limitation, consent requirements, and transfer restrictions. The legal question is how much flexibility can be preserved while remaining compliant.

Commercial Feasibility

Not all legally permissible data uses are commercially viable, and not all commercially attractive uses are legally permissible. Counsel must evaluate whether legal constraints (e.g., requiring robust consent or limiting secondary use) will undermine the business case and advise on compliant alternatives.

Brand, Trust & Accountability

Privacy violations can cause lasting reputational harm, eroding consumer trust, triggering regulatory scrutiny, and inviting litigation. Even when a data use is technically lawful, counsel should assess whether it aligns with the organization's public privacy commitments and stakeholder expectations.

STEP 1: DATA FLOW DECISION POINTS

PURPOSE: Use these questions to map data characteristics before evaluating legal obligations. Answer each to identify applicable laws, roles, and restrictions.

WHERE TO START? Map the data before you assess the law. Each question below surfaces a dimension that determines which obligations apply.

What privacy laws might apply?

State, federal, sector-specific — HIPAA, CMIA, state privacy laws

Are there restrictions on use or disclosure?

Contractual, regulatory, or consent-based limitations

What personal data is involved?

Identify data types; determine if sensitive categories apply

Is the data sensitive?

Part 2, race/ethnicity, biometric, financial, or health-related data

What is the client's role in processing?

Controller/CE vs. processor/BA — determines legal obligations

What data retention requirements apply?

Period, format, and jurisdiction-specific rules

What is the context of collection?

Identifiable, pseudonymized, or anonymized? LDS vs. de-identified?

What jurisdictions apply?

State privacy laws? HIPAA? CMIA? EU/UK GDPR?

What is the data source?

Internal, data broker, research study, government, or data subject?

"Getting to Yes" — Step 1: Key Data Questions

Three threshold questions to assess data usability before deeper analysis begins.

1 Do you really need identifiable or sensitive data?

- Use de-identified data where scientifically or operationally adequate.
- Avoid Specially Protected Information (SPI); otherwise, consent may be required.
- Steer clear of "higher risk" jurisdictions when data collection is discretionary.

2 Do you have rights to the data?

- Prefer existing internal data over acquiring new data sources.
- Position your client as controller/covered entity rather than processor/business associate where feasible.
- Obtain appropriate licenses, representations, and warranties from third-party data providers.

3 Can you trade "data flexibility" for lower compliance costs?

- Evaluate whether broader data use rights are worth the compliance overhead they require.
- A narrower, clearly-scoped use often reduces legal risk and accelerates approvals.

"Getting to Yes" — Step 2: Use Case Questions

Evaluate legality, scope, and flexibility of the proposed data use.

1 Is it a new use case?

- Group into an existing approved use case if scope permits.
- Fit within existing disclosure or contractual permissions.
- Use "just in time" notice or consent if a new permission layer is needed.

2 Is the use case highly regulated?

- Avoid highly regulated categories where possible (e.g., FDA-regulated SaMD, research).
- Is it really AI — or analytics? Is it really intended to treat/diagnose — or informational?
- Is it really a "sale" or "sharing" — or internal processing?
- Is it really "automated decision-making" — or providing options to a human decision-maker?
- Is it really "research" — or health care operations/population health?

3 Can you tweak to leverage data exchange rules?

- Proactively leverage TEFCA/Carequality frameworks to enable permissible health data exchange.

"Getting to Yes" — Special Considerations: AI Use Cases

Four dimensions to evaluate when AI is involved in data processing.

1 What data will the vendor have?

Use de-identified data wherever possible. Avoid exposing proprietary, confidential, or patient-level information to third-party AI vendors unless contractually protected.

2 What is the use case?

Avoid "automated" decision-making and potential discrimination risk — particularly in HR-adjacent applications where "significant" decisions trigger ADMT obligations. Build in prompt iteration to refine and improve outputs.

3 How can the vendor use your data?

Prohibit secondary uses — especially model training using your proprietary data. This must be expressly addressed in vendor agreements. Silence is not sufficient.

4 What risk mitigations are in place?

Implement strong governance, training, and technical controls (e.g., blocking access to public AI tools). Provide notice and opt-outs where applicable. Maintain a backup plan if AI processing is unavailable or challenged.

"Getting to Yes" — Special Considerations: Cookies & Tracking

Four questions to structure cookie compliance analysis.

1 What is the business risk tolerance and ROI on cookies?

- Disable cookies that do not add meaningful business value — they create legal exposure without corresponding benefit.

2 What data is collected or transmitted?

- De-identify data or obtain expert de-identification certification.
- Avoid collection or transmission of health data or PHI through cookie technology.
- Consider using synthetic or proxy data instead.

3 What do existing contracts say?

- Ensure compliance with Customer-to-Platform (C2P) terms, Data Processing Agreements (DPAs), and Business Associate Agreements (BAAs).

4 What alternatives exist?

- Evaluate privacy-preserving alternative technologies (e.g., server-side tracking, consent management platforms).
- Move data processing in-house to reduce third-party sharing.

Step 3: Commercialization Strategy

Key questions to evaluate before bringing a data product or service to market.

1 How will the product be marketed?

Consider FDA, FTC, and Medicare regulations on marketing content and claims. Who will review and update marketing materials?

↓

2 What agreements are required?

DPA, DUA, BAA, NDA, Data Sharing Agreement, HIE Participant Agreement — match agreement type to data type and relationship.

↓

3 Who is the data recipient, and how will they use it?

Is the transfer a "sale" under applicable privacy law? What downstream uses are intended or foreseeable?

↓

4 What do the agreements actually say?

Privacy/security obligations, IP and data ownership rights, liability limitations and disclaimers — specificity matters.

↓

5 Has privacy and security due diligence been conducted?

Before sharing data with a third party, complete vendor due diligence — security assessments, data mapping, and contractual protections.

"Getting to Yes" — Step 4: Risk & Commercialization Issues

Two risk-mitigation levers to reduce legal exposure at the commercialization stage.

1 Can the risks be outsourced?

- Shift legal risk through well-drafted contracts — indemnification, representations, and warranties.
- Use consent forms to transfer responsibility from the organization to the data subject where appropriate and lawful.
- Ensure contractual risk allocation is realistic and enforceable, not merely aspirational.

2 Can risks be managed by adjusting the commercialization strategy?

- Restructure the offering to avoid FDA regulation — for example, by clarifying that a product is informational rather than diagnostic.
- Tone down feature descriptions to reduce regulatory and litigation risk (e.g., avoid overclaiming AI capabilities).
- Structure as B2B rather than direct-to-consumer to trade data flexibility for lower privacy law exposure.
- Evaluate whether a narrower commercial scope meaningfully reduces legal risk without eliminating business value.

STEP 5 · GOVERNANCE MATURITY

Efficiently Addressing Risks Through Governance

Your governance maturity level determines how fast and smoothly you can say "yes" to new AI use cases.

BASELINE

Reactive · Risk-Based

What this looks like:

- You respond to problems after they happen — not before.
- Only the highest-risk use cases get attention.
- Processes are informal and change frequently.
- Hard to repeat or scale what works.

⚠ **Slower approvals. More surprises. Higher risk exposure.**

DEVELOPING

Anticipatory · Incomplete

What this looks like:

- Some standard processes exist, but not everywhere.
- You're starting to think ahead — but gaps remain.
- Example: You flag notice/consent issues early for new use cases, but you don't yet have a centralized tracking system.
- Some consistency, but still ad hoc in places.

→ **Better than baseline, but still friction and blind spots.**

MATURE

Prepared · Proactive

What this looks like:

- Processes cover the full lifecycle — from intake to go-live.
- Everyone knows their role. Reviews are defined and documented.
- Examples: Consent management systems, standard PIA/DPIA procedures, cross-functional sign-off workflows.
- Predictable outcomes. Legal isn't a bottleneck — it's a partner.

✓ **Less friction. Fewer surprises. Faster path to market.**

Step 6: Feedback Loop — Part 1 of 2

Each completed engagement feeds back into five core governance program areas.

Data Provenance & Lineage

Document data origins, transformations, and flows. Each new use case should update data maps and provenance records — building an auditable chain of custody.

When regulators or litigants ask "where did this data come from?", provenance records are your answer.

Record Retention

Confirm and apply jurisdiction- and data-type-specific retention schedules. Update policies when new data categories or jurisdictions are implicated.

Retention failures are a key source of regulatory findings. Each engagement is an opportunity to verify and correct.

Data Minimization

Use each engagement to reassess whether data collected is still necessary and proportionate. Flag opportunities to reduce data scope in future projects.

Minimization reduces breach exposure, simplifies consent, and demonstrates good faith to regulators.

Contracts

Capture new or revised contractual obligations in the contract management system. Flag templates that need updating based on regulatory changes or deal learnings.

Silence in a contract is not a defense. Every engagement surfaces gaps that templates should address prospectively.

Privacy Notices & Consents

Identify when a data use requires a notice update or fresh consent. Trigger the MLR/legal review process and update the notice inventory accordingly.

Stale or incomplete notices are among the most common enforcement triggers. Use each engagement to pressure-test currency.

Each completed legal engagement is an input into the governance program — updating policies, contracts, notices, and data maps.

STEP 6 · FEEDBACK LOOP

The Continuous Improvement Cycle

How governance gets stronger with every engagement.

01 **New Use Case Identified**
Business team brings a new data initiative to Legal & Compliance for review.

02 **Legal & Privacy Analysis**
Counsel evaluates data type, role, jurisdiction, use case, and commercialization plan.

03 **Decision & Documentation**
Findings recorded: approved, approved with conditions, or declined. Reasoning documented.

04 **Governance Program Update**
Provenance, retention, minimization, contracts, and notice records updated.

05 **Refined Guidance Issued**
Updated templates, FAQs, and pre-approved use cases published for faster future engagements.

To Sum Up

Five principles for effective data privacy legal practice

1 **Build on what exists**

Start with basic compliance tools, pre-approved use cases, and existing governance guidance — don't reinvent the wheel for every engagement.

2 **Flexibility changes the analysis**

How a use case is structured — what data, what role, what purpose — can meaningfully shift legal risk. Flexibility is a legal tool.

3 **Define priorities and trade-offs**

Not every legal concern has equal weight. Understand the client's risk tolerance and identify which compliance investments are non-negotiable vs. optional.

4 **Make it a team sport**

Privacy legal analysis requires collaboration across legal, compliance, IT, and business. Plan for involvement from all stakeholders — and for the governance program to evolve.

5 **Avoid easy facts for regulators**

Structure products, marketing, and data flows to avoid creating clear-cut regulatory violations. Ambiguity is sometimes protective; clear violations never are.

KEY REMINDER

- Privacy analysis is not binary. The goal is structured risk management, not elimination of all risk.
- Getting to "yes" is the job — but only a legally defensible "yes."
- Document your reasoning. Legal analysis that isn't recorded is analysis that didn't happen.
- The governance feedback loop is how organizations get smarter over time. Every engagement is an input.

DATA MINIZATION - LIMIT WHAT YOU COLLECT

Five rules for collecting only the data you truly need.

Collect for a Specific Purpose

Know why you need each piece of data. Do not collect what you don't need. Example: Skip mailing addresses for email campaigns.

Use De-Identified Data

Wherever possible, remove names and identifiers. Only use personal data when truly required.

Find Ways to Collect Less

Ask: Can we reach this goal with less data? Example: Use a checkbox to confirm age instead of collecting a birth date.

Use Data You Already Have

Check existing records first. Avoid collecting the same data twice. Example: Reuse sign-up emails for campaigns.

Limit Open Text Fields

Avoid wide open text boxes unless needed. Limit the space to reduce unnecessary input. Large text fields create extra compliance work.

DATA MINIMIZATION - LIMIT HOW YOU USE DATA

Five rules for managing and protecting data after you collect it.

Collect Less Often

Avoid collecting data in real time unless necessary. Periodic collection is often enough. Example: Gather location every 5 - 30 minutes instead of continuously.

Delete Data Promptly

Delete unnecessary data quickly. Do not let it flow into larger databases, especially where you cannot stop continuous data feeds at the source.

Audit Tracking Tools Regularly

Review all cookies and tracking technologies regularly. Remove any that are no longer needed and delete the data they collected.

Audit Data Feeds Regularly

Check data feeds often to make sure they only include what is still needed. Watch for changes in data elements, frequency, or third-party content.

Restrict Access and Use

Limit who can see and use personal data. De-identify, mask, or tokenize where possible. Prevent data from flowing into systems that don't need it.

DATA MINIMIZATION

QUICK REFERENCE — 10 RULES AT A GLANCE

COLLECT

1 Collect for a Specific Purpose

Only gather data that is directly needed for a defined, documented purpose.

2 Use De-Identified Data

Anonymize or de-identify wherever possible before collecting or sharing.

3 Find Ways to Collect Less

Challenge every data field — if it isn't essential, remove it from the flow.

4 Reuse Data You Already Have

Check existing datasets before initiating a new collection effort.

5 Limit Open Text Fields

Replace free-text inputs with structured options to reduce unintended data capture.

USE & RETAIN

6 Collect Less Often

Periodic collection beats real-time when possible — reduce frequency to reduce exposure.

7 Delete Data Promptly

Remove unnecessary data before it spreads to downstream systems or third parties.

8 Audit Tracking Tools

Remove cookies, pixels, and tracking scripts no longer actively needed.

9 Audit Data Feeds

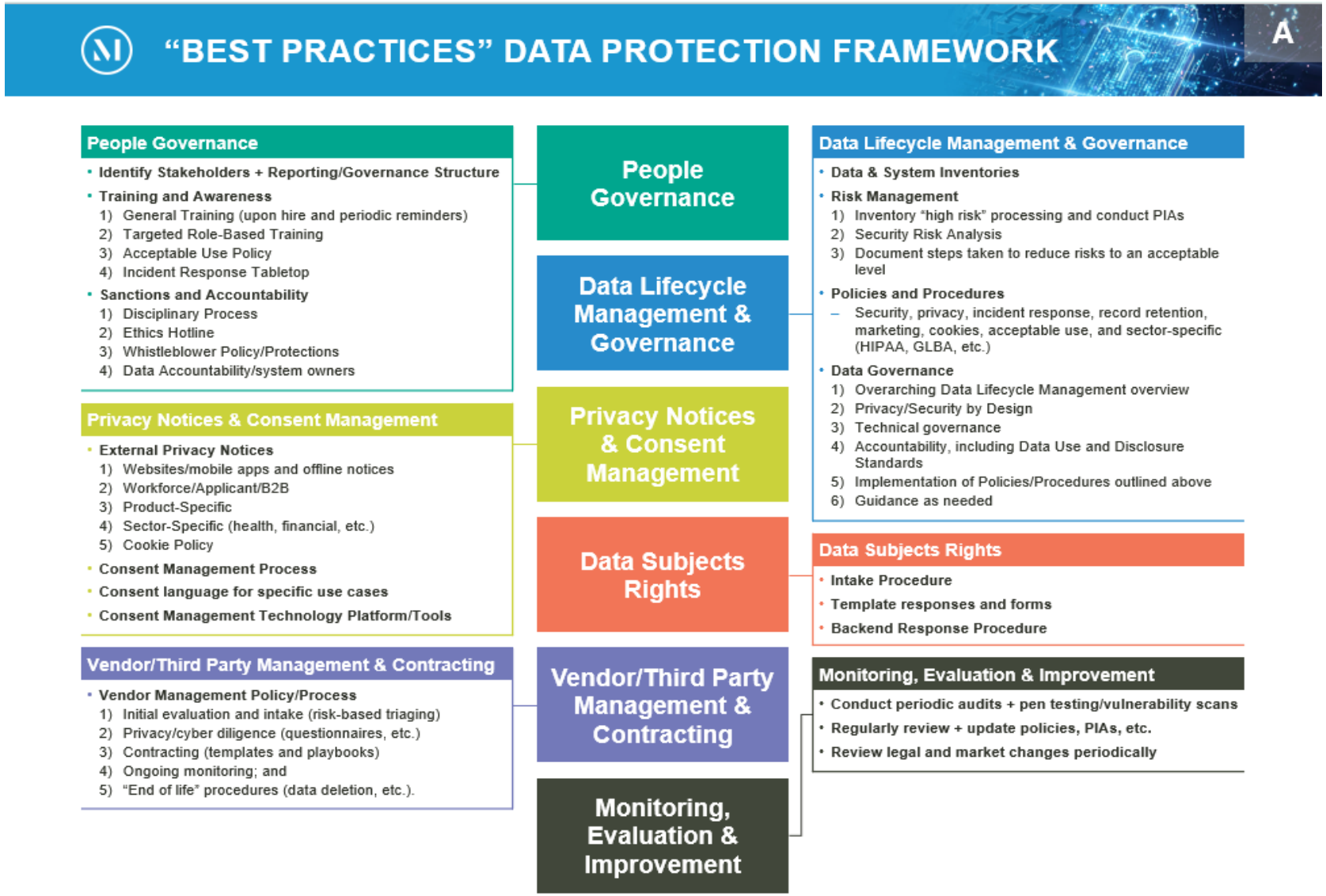
Periodically check inbound feeds for unexpected fields or changes in data content.

10 Restrict Access and Use

Mask, tokenize, or apply role-based access controls to limit who can see personal data.

TIP *When in doubt, collect less — it's easier to add data later than to delete it after a breach or audit.*

DATA GOVERNANCE "BEST PRACTICES"



McDermott Will & Emery

QUESTIONS

ELLIOT GOLDING

McDermott Will & Schulte

Egolding@mwe.com

JOANNE CHARLES

Gilead Sciences

Joanne.Charles@gilead.com

AMY PAPSUN

Headway

Amy.papsun@findheadway.com

THANK YOU!