PROGRAM MATERIALS
Program #35117
September 10, 2025

State Privacy and AI Law Updates

- Alan Friel, Esq. - Squire Patton Boggs
- Sam Marticke, Esq. - Squire Patton Boggs
- Colleen Yushchak - Ankura Consulting Group, LLC.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

State Privacy and AI Law Updates

September 10, 2025

Presenters

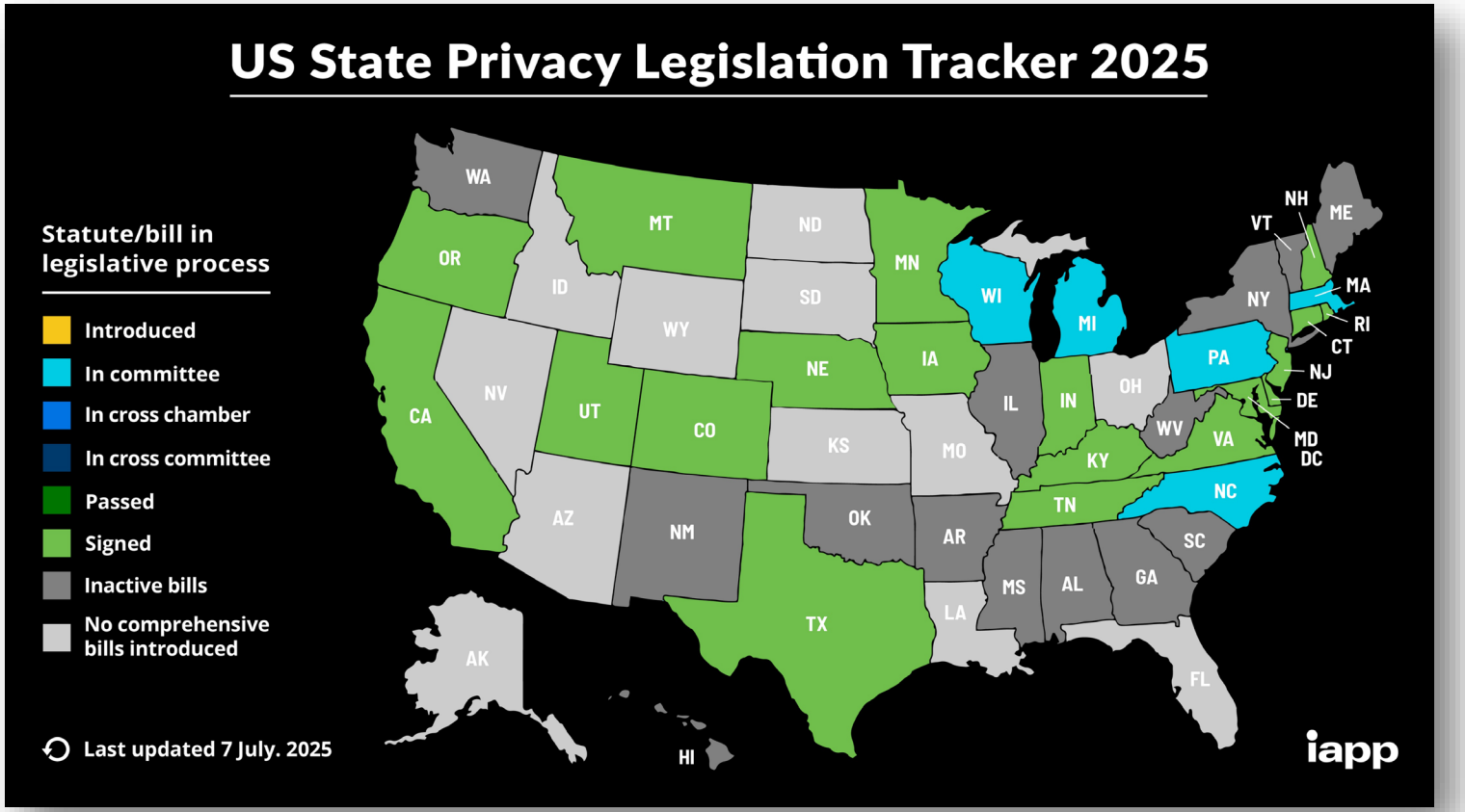
Alan Friel
Squire Patton Boggs
Partner, Global Chair
Data Privacy, Cybersecurity, & Digital Assets

Samuel Marticke
Squire Patton Boggs
Associate,
Data Privacy, Cybersecurity, & Digital Assets

Colleen M Yushchak
Ankura
Senior Managing Director
Lead of Global Privacy Practice

State Privacy Laws

- **20** states have enacted omnibus privacy laws
- **15** in effect, remaining 5 throughout ‘25-26



Source: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

State Consumer Privacy Law (CPL) Applicability

ankura SQUIRE PATTON BOGGS

California

- "Do business (for profit)" in state
- Meet one of three thresholds
  - Gross global annual revenue over $25 million
  - Buy, sell, or share the personal information of 100,000 or more California residents or households; or
  - Derive 50% or more of their annual revenue from selling California residents' personal information
- Covers consumers, B2B contacts, employees, applicants, contractors

Other states*:

- "Do business" in state OR produce products/services targeted at state residents, AND
- Collect/process certain # of state residents' PD (typically 50k to 100k) *(there are some nuances to this)*
  *Some states do not have # thresholds (NE, TX)
- Generally, cover only traditional consumers
- Some cover non-profits

Covered Data

- **Personal information** or **personal data** is broadly defined as information that identifies or can identify, or is linked or reasonably linkable to an identified or identifiable natural person.

- Personal information does not include information that is publicly available, deidentified, or (in CA) aggregated.
  - But does cover inferences based thereon

- California identifies specific categories of personal information:
  - Identifiers, such as name, address, IP address, email, passport number, etc.;
  - Personal records, such as name, phone number, and other identifiers;
  - Commercial information, including records of property, products, or services purchased;
  - Biometric information;
  - Internet or other electronic network activity;
  - Geolocation data;
  - Sensory data, such as audio, electronic, visual, thermal, or similar information;
  - Professional or employment-related information;
  - Education information that is not publicly available;
  - Sensitive personal information (separately defined);
  - Inferences drawn from any of the above.

Sensitive PI/PD

"Sensitive personal information" means:

(1) Personal information that reveals:

(A) social security, driver's license, state identification card, or passport number.

(B) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) precise geolocation.

(D) racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

(E) contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) genetic data.

(G) neural data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

- Opt-out: CA, UT, IA
- Opt-in: Remainder of states
- Subject to processing exceptions
  - Requested services
  - Security
- Maryland
  - No sales of sensitive information
- TX and FL
  - Special notice for sale of sensitive
- CA and OR considering banning sales of location data
- CO requires deletion or inoperability if consent is withdrawn

Key Features of State Privacy Laws

- Privacy Policies content requirements
  - Especially CA and CO
  - + CA “pre-collection notice” requirements
- Data and Entity level exclusions
- Specific contract language with service providers/processors; CA has contract requirements for “sale” recipients
- Data subject rights
- Non-discrimination (except Utah)
- Data protection/risk assessments
  - Except Iowa and Utah
- Data security requirements
- Data minimization and proportionality of use (no secondary uses)

Unique Features

- Minnesota:
  - CPO and data mapping
- California:
  - Cybersecurity audits
  - Data inventory and third party tech assessment requirements
- Connecticut
  - Consumer Health Data (CHD) Controller
    - Controls data about physical or mental health including gender affirming care, reproductive health, or sexual health care
  - WA and NV have stand-alone CHD laws
- Colorado
  - Extensive biometric processing requirements
    - Including in HR context
- Tennessee
  - NIST affirmative defense
- Differences in consumer rights
- Different treatment of children and teens

Data Subject Rights

- Right to **confirm whether controller is processing** the consumer's personal data and **access** the data
- Right to **correct** inaccuracies in consumer's personal data
- Right to **delete** personal data *provided by* or *obtained about* the consumer (varies by state)
- Right to **data portability** (provided controller not required to reveal a trade secret or violate others' privacy)
- Right to **opt-out** of the processing of the personal data for purposes of **targeted advertising** and certain **profiling** and **ADMT** (CA)
  - Unless, for profiling/ADMT, appeal (CA) or human intervention (CO)
- Right to **opt-out of sale and sharing for targeted advertising** (CA – "CCBA")
- Right to **obtain a list of (specific or categories of) third party recipients** of personal data (handful of states)
- Right to **question the result of profiling** (MN) and **access ADMT** info (CA)
- **Limit Sensitive PI** processing (CA) (FL)

Access and Confirm Processing Rights

- All U.S. State Privacy Laws provide a right to access PI/PD
- California right of access requires of:
  - Categories of third parties receiving disclosure of PI
  - Categories of third parties receiving sales of PI
- Colorado requires list of all third parties to whom controller disclosed biometric information
- RI online service PII sales recipient disclosure in online notice

- All U.S. State Privacy Laws require controllers to provide information about third-party recipients of the data.
- Generally a "disclosure" is different than a "sale" and disclosures between two controllers without a direct consumer interaction might be deemed a disclosure to a third party even if not a sale
- Four of the State Privacy Laws (Oregon, Delaware, Maryland, and Minnesota) specifically require controllers to provide a right to obtain a list of either **specific** third parties or **categories** of third parties

Right to Access/Portability

- Most state privacy laws contain the right to obtain a copy of data
- CA has a unique lookback provision
- A few states limit portability to personal data processed by automated means
- No obligation to retain just for future consumer access
- States with portability requirements require controllers to provide copies in a usable format
- Colorado: additional information required for responses to access requests if the request includes biometric information
- Exceptions
  - Trade Secrets
  - Disproportionate Effort
  - Privilege
  - Rights of others

Right to Correct

- All U.S. State Privacy Laws (except Utah and Iowa) provide a correction right for consumers
- Implementation requirements are not clear in most states
- Indiana's right to correct only applies to information provided by the consumer to a controller
- Florida allows denials if a controller uses a self-service mechanism

- California
  - Does NOT extend to PI that belongs to or is maintained on behalf of another person
  - Businesses must consider the totality of the circumstances to decide whether a correction is needed
  - Must instruct service providers to correct within their systems
- Colorado
  - Generally, includes similar requirements to California
  - Does not enumerate factors for the totality of circumstances test

Right to Delete

- All U.S. State Privacy Laws create rights to delete, subject to very broad legitimate purposes exceptions
  - CA, UT and IA only if collected from the consumer
  - Responsible for SP/P deletion
  - Legitimate retention exceptions, but only for so long as the exempt purpose continues
- California's requires passing down deletion requests to third parties if the initial disclosure was a "sale" or "share"

California Data Broker Delete Request and Opt-Out Platform (DROP) Regulations

- California
  - requires data broker registration, published on state website
  - will launch a single consumer opt-out request mechanism, which data brokers must check and delete PI of any consumer that matches As of 2025, just under 500 entities are registered as a data broker
- CA developing a state-run global opt-out system
- Texas recently amended its data broker law to broaden applicability and increase requirements for data brokers
- Other states have less robust data broker laws
  - NV, VT, and OR
- Vermont and Texas include cybersecurity requirements in their registration laws
- Significant enforcement action in CA, OR and TX

Right to Opt-Out Sale/Share/Target

- Most state privacy laws grant consumers a right to opt-out of the sale of their personal information
- California additionally allows consumers to opt out of the *sharing* of their personal information for CCBA
  - Proposal to expand for also "behavioral advertising pulled
- The other states apply opt-out to processing for "targeted advertising"
- States vary regarding use of Opt-out Preference Signals (OOPS) or Universal Opt Out Mechanisms (UOOM)
- Cookie challenges
- Symmetry of choice
- IAB MSPA signal program
- Opt-in for "children" / "teens"

Privacy Law Enforcement Risks

- CPPA:
  - **$632,500** civil penalty to Honda for violations of data subject rights provisions
  - **$345,178** civil penalty to clothing retailer Todd Snyder for failure to process opt-outs
- CA AG :
  - **$1 million** civil penalty to Sophora for cookie issues
  - **$1.55 million** civil penalty to Healthline.com for failure to process opt-outs and failure to adhere to purpose limitation principles
- Other California enforcement actions include:
  - **$46,000** against a Florida databroker for failure to register with the Agency
  - An agreement with a California databroker to **shut down in CA**
- Texas recently filed the first lawsuit under a state privacy law against Allstate for collecting information from drivers without their consent.
- Texas also reached a **$1.4 billion** settlement with Meta for its collection of biometric information without informed consent.

CA New and Amended Regulations

- California's CPPA is currently in the final stages of rulemaking for implementing regulations regarding ADMT, risk assessments and cybersecurity audits.
  - On July 24, the Board approved the draft regulations.
- As currently proposed to be scheduled:
  - ADMT requirements – Jan 1, 2027
  - Security Audits – Depends on size of business
    - April 1, 2028: $100 million+ in gross revenue
    - April 1, 2029: between $50-$100 million in gross revenue
    - April 1, 2030: under $50 million in gross revenue
  - Data Processing Risk Assessments:
    - Activities occurring on or after effective date [October 1 or Jan 1] are subject to risk assessments
    - Documentation for activities before effective date but continuing after, not required until December 31, 2027 and filing due on April 21, 2028
  - Other amendments – as of effective date

Applicability

Automated decision making technology processing PI

&

Used for a significant decision concerning a consumer

Definition of "Automated Decisionmaking Technology" (ADMT)

- "any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking."
  - "Substantially replace" means "a business uses the technology's output to make a decision without human involvement."
  - Human involvement is defined as requiring the human reviewer to:
    - Know how to interpret and use the technology's output to make a decision
    - Review and analyze the output of the technology and other information that is relevant to make or change the decision; and
    - Have the authority to make or change the decision based on their analysis.

“Significant Decisions” – “~~access to, or~~ provision of denial of:

Health Care Services	Financial or Lending Services	Employment Opportunities or Compensation
Education Enrollment or Opportunity	Insurance	Housing

New ADMT Requirements

Pre-Use Notice

Right to Opt-Out*

~~Notice of Adverse Decision~~

Right to Access

** Subject to exceptions such as permitted uses or if human appeal is offered*

Risk Assessments

- Most of the state privacy laws require that Data Privacy Impact Assessments (DPIAs) of "high risk" data practices are documented and available for inspection
  - Only Iowa and Utah do not contain this requirement
  - MN and CA (as part of 7123(b)92)(E) auditing) require data inventories
- Common elements (+ certain autoprocessing for inferences and training data in CA):
  - Assessments must be performed before the processing activity occurs
  - Consider the following categories of risks:
    - Sale / target / sensitive data processing
    - Profiling that presents risk of
      - Unfair or deceptive treatment of consumers
      - Unlawful disparate impact on consumers
      - Financial, physical, or reputational injury to consumers
      - A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person
      - Other substantial injury to consumers

Risk Assessments

- Colorado (effective July 1, 2023)
  - The depth, level of detail, and scope will depend on the scope of the processing activity's risk, controller's size, and other factors, but:
    - 12 explicit inquires
    - 12 additional if profiling
  - Involve all relevant internal stakeholders
  - Update the assessment as appropriate considering the processing activity (at least annually for profiling)
  - Provide to AG within 30 days of a request

- California
  - Must consider:
    - Categories of personal data (including sensitive personal information) processed
    - Operational elements of processing
    - Purposes of the processing
    - Benefits and negative impacts associated with processing (but not required to be included in the risk assessment report open to inspection)
    - Safeguards to address the negative impacts

AI-Specific Laws

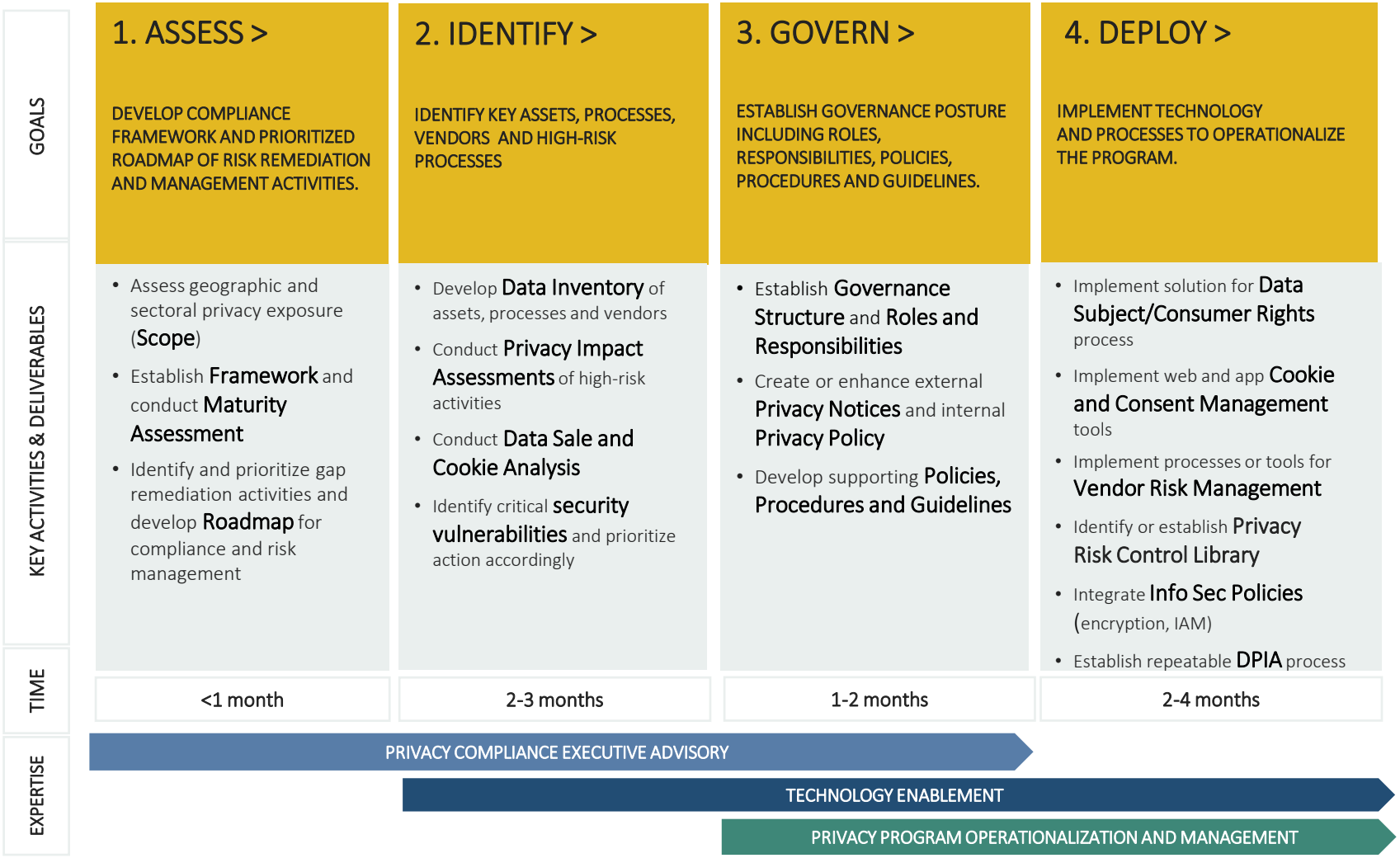
- **CA AI Training Data Transparency Act (Civil Code Sec. 3110)**
  - On or before 1/1/26, for Gen AI released on or after 1/1/20:
  - Developers must publish details on how it was trained
  - No risk assessment details
  - No error or bias testing
- **CA Bot Disclosure**
- **CA AI Transparency (watermark)**
- **UT AI Disclosure (5/1/24)**
- **Product Liability**
- **Federal pull-back**

- **CO AI Act (eff. 6/30/26)**
  - Deployers and Developers of HAIS have duties of care to protect from algorithmic discrimination
  - HIAS makes or substantial factor in consequential decision
    - Material legal or similarly significant effect
  - Risk Management
    - Program
    - Assessments
    - Predeployment and Adverse Decision Notices for HIAS and basic notice of other AI

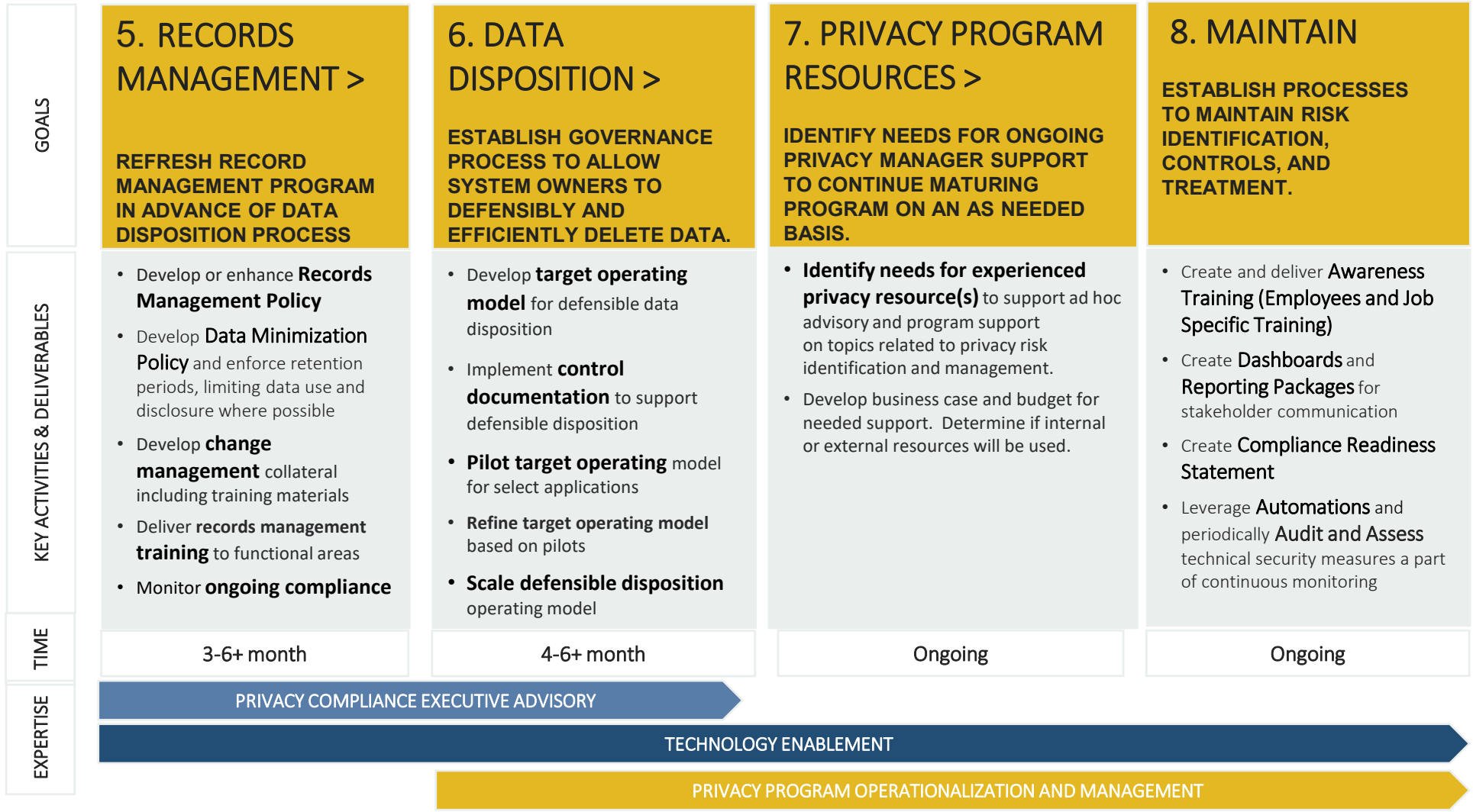
HR and AI

- California
  - CCPA ADMT and Assessments
  - CA Civil Rights Council
    - As of Oct 1 must assess and prevent bias
    - Failure to do so can support discrimination claims'
    - No opt-out
  - IL 103-0804 (HB 3773)
    - As of 1/1/26 cannot use AI in a manner that discriminates in employment
    - Usage notice required
  - IL AI Video Interview Act
    - Notice of use and how it works
    - Consent requires
  - NYC Local Law 144
    - Bias assessment for use for covered decisions
    - 'Pre-use notice required

Operationalizing a Privacy Program



Operationalizing a Privacy Program



What is a Data Inventory?

Asset Assessments

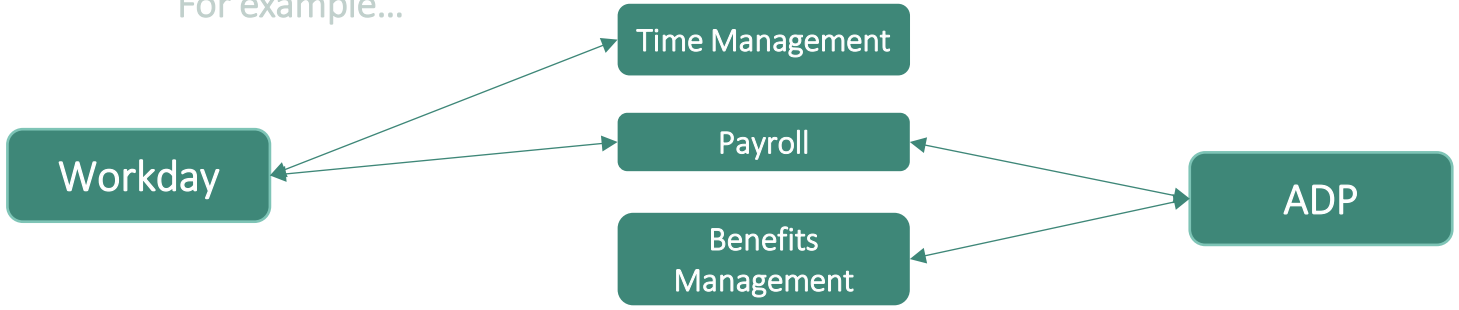
- An **asset** refers to a system owned or leveraged by the organization that collects, stores or processes personal data. (e.g., Application, website, database, etc.)
- *Ex. CRM systems, HR systems, shared drives, social media accounts, finance systems, online advertising platforms and data warehouses.*
- Typically assigned to **Technical Owners**

Processing Activity Assessments

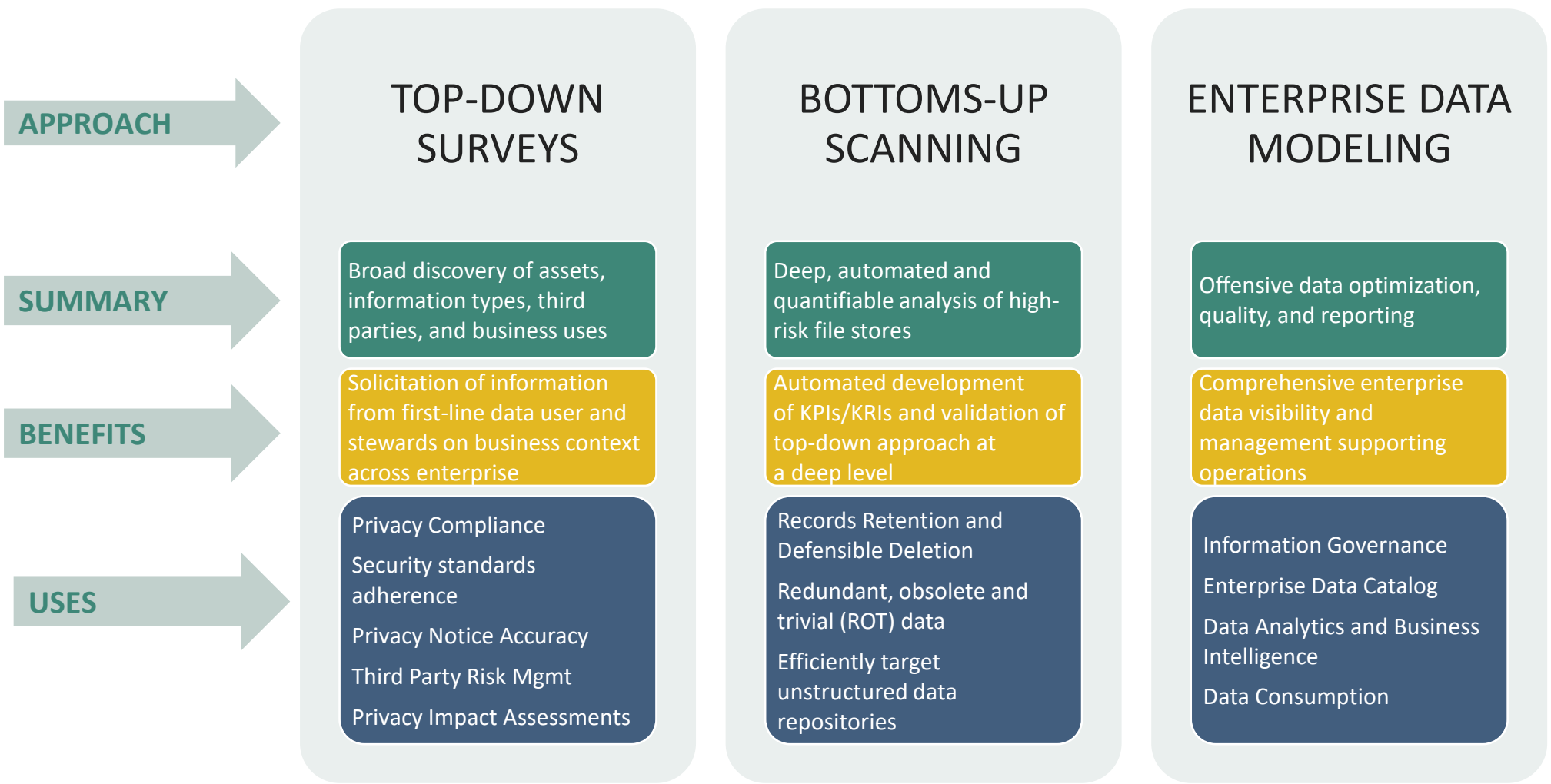
- A **processing activity** refers to any operation performed on personal data (whether those operations are automated or not).
- *Ex. Accounts Payable, Recruiting, Social Media Marketing and Lead Generation.*
- Typically assigned to **Business Owners**

Assets and Processing Activities is a many-to-many relationship:

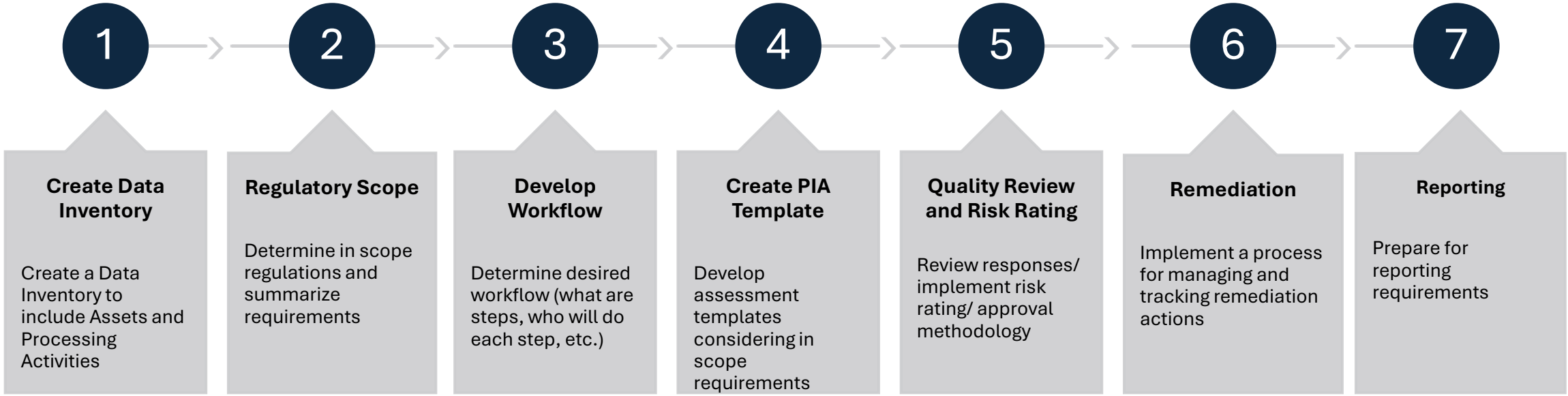
For example…



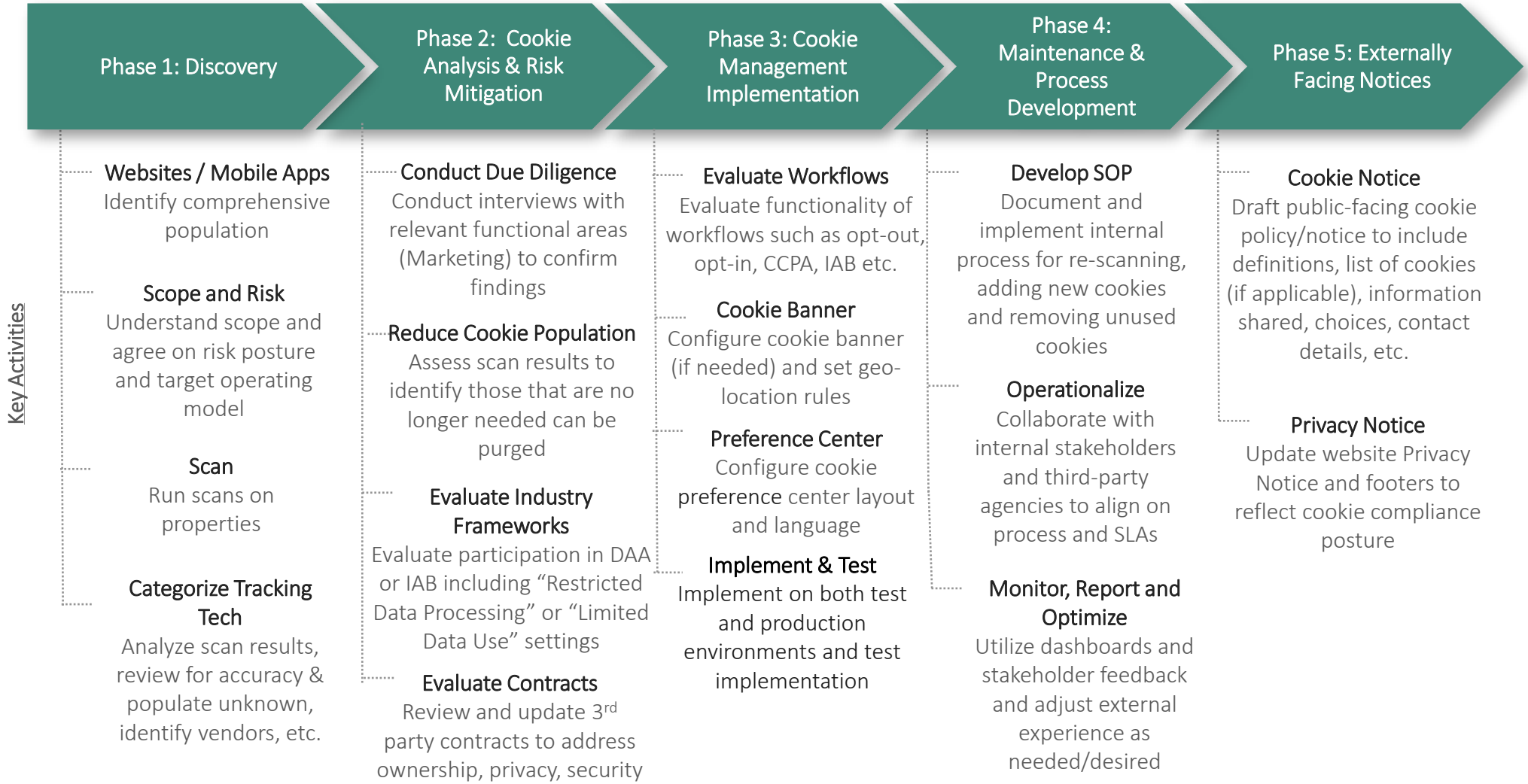
Approaches to Create a Data Inventory



Operationalizing Data Privacy Assessments



Operationalizing Tracking Technology Compliance



Operationalizing Consumer Rights Request Process

ankura SQUIRE PATTON BOGGS

USE DATA INVENTORY TO:

- Identify unique assets that contain personal information.
- Work with legal team and outside counsel to review legal exemptions for each asset based on data and use.
- Work with Business Owners to review operational exemptions for each asset and to understand level of overlap of personal information between assets.
- Understand data subject types, data subject locations and relationships to company.

DEVELOP COLLECTION POINTS

- Create web form for consumers to exercise rights.
- Identify and include identity verification process in web form.
- Implement alternate request mechanisms including email and toll-free phone number).
- Update Privacy Policy Notice, collection points, etc. as required based on request mechanisms and navigation on website(s).

CONFIGURE WORKFLOWS

- Create workflow including operational touchpoints and communications with roles and responsibilities identified in adjudication process.
- Create response/ communication templates.
- Automate process, workflows and templates in privacy tool

DEVELOP PROCEDURE

- Confirm and document operational step-by-step procedures with narratives and roles and responsibilities for request adjudication including identity verification or confirming exemptions or denial of requests.
- Operationalize process and procedure

TABLE-TOP TESTING

- Run table-top testing on different request scenarios.
- Update workflows and/or procedures and platform as result of tests.
- Publish and go live.

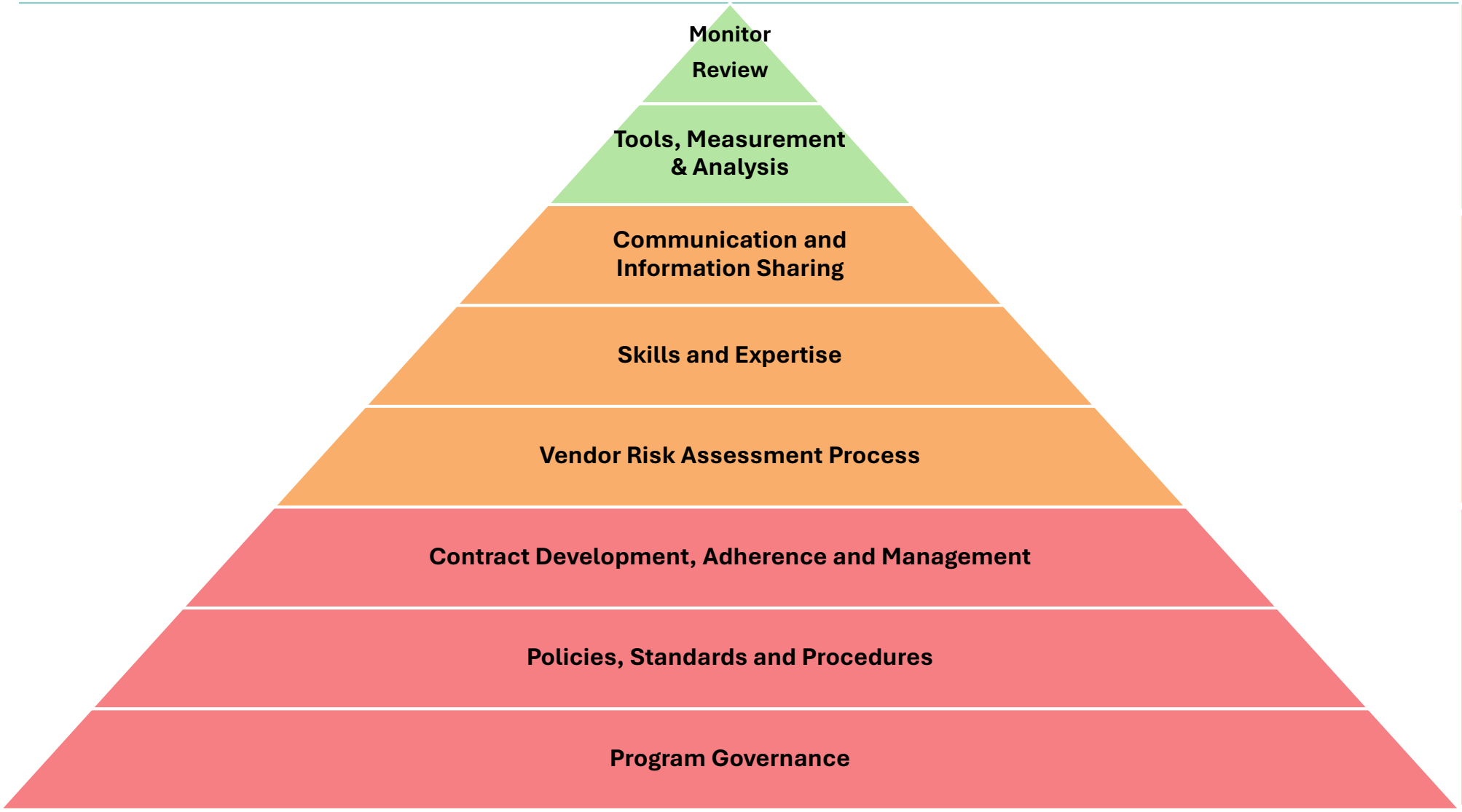
TRAINING AND TRANSITION

- Develop and conduct training for process owner, software administrator and team members managing procedure for requests.

Operationalizing Vendor Risk Management

1. Evaluate Current Vendor Risk Management Maturity
2. Develop Target Operating Model
3. Develop Action Plan

Step 1: Evaluate Vendor Risk Management Maturity

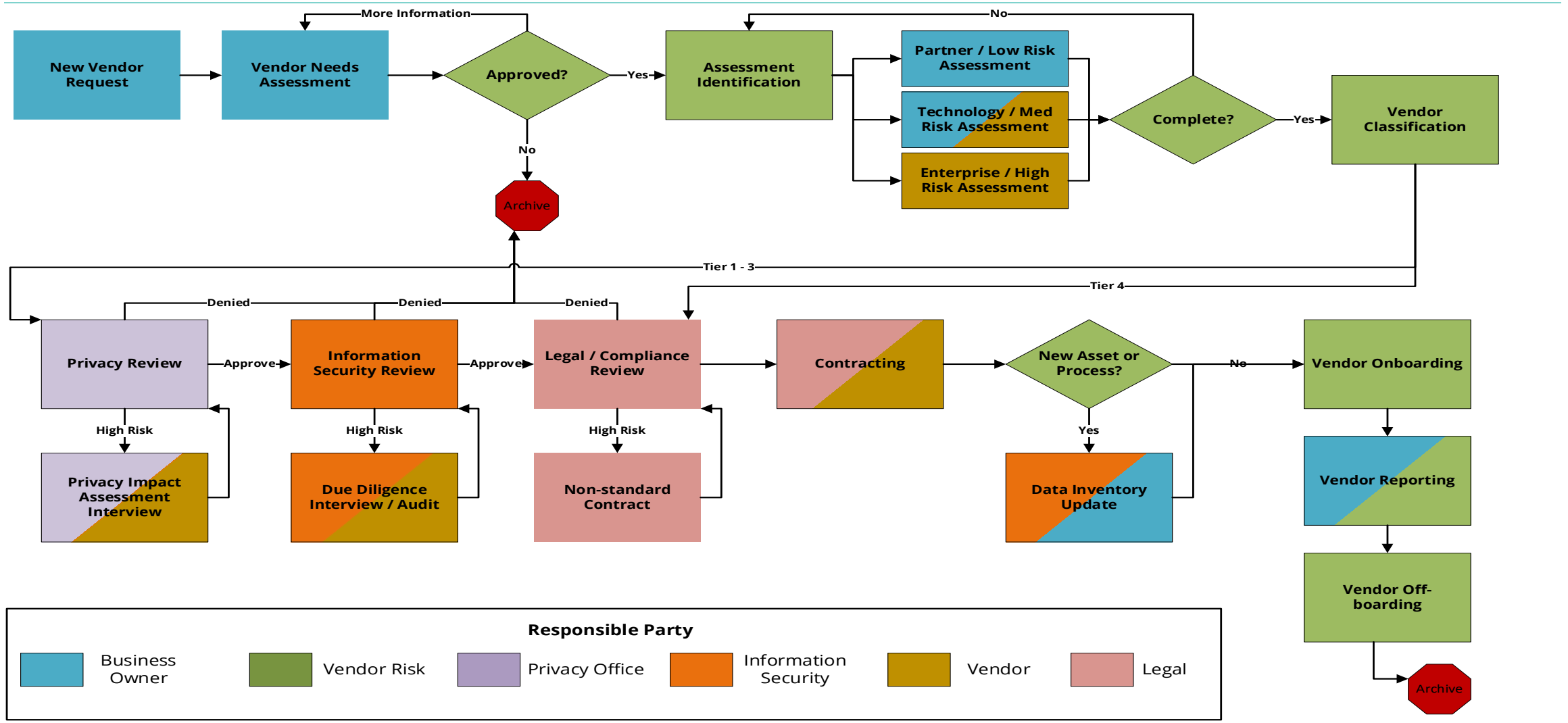


Maintain
2 Categories
11 Subcategories
52 Criteria

Operationalize
3 Categories
16 Subcategories
85 Criteria

Build
3 Categories
16 Subcategories
95 Criteria

Step 2: Develop Target Operating Model



Step 3: Develop Action Plan

	Identify	Develop	Implement	Maintain
Activities	➢ Gather and standardize vendor sources (e.g., accounts payable, contracting systems, data inventories, etc.) ➢ Review existing questionnaires, policies, procedures and processes involved in VRM lifecycle ➢ Evaluate current level of maturity and priorities for improvement	➢ Define risk framework of risk areas, likelihood, impact, default controls and control strengths ➢ Review, standardize and rank existing vendors ➢ Engage across IT, Info Sec, Privacy, Legal to develop the workflow and Target Operating Model ➢ Evaluate technology ➢ Draft policy and procedure	➢ Communicate roles and responsibilities ➢ Test and deploy technologies and processes ➢ Deliver job-specific training ➢ Provide broader employee communication plans	➢ Develop and implement KPI and KRI dashboards for program management ➢ Develop board reporting processes and scorecards ➢ Establish processes for on-going vendor reviews and off-boarding ➢ Conduct periodic assessment of people, process, and technologies
Artifacts	➢ Standardized vendor list ➢ Maturity assessment and roadmap	➢ Target operating model ➢ VRM Policy and Procedure	➢ VRM Workflow tool ➢ Training decks ➢ Employee communications	➢ VRM Dashboard ➢ Executive scorecard ➢ Review and off-boarding procedures

Implementing an AI Management Program

ankura

SQUIRE PATTON BOGGS

Create AI System Inventory

Develop inventory of AI systems which documents the AI System Name, AI System Owner, System Description, other descriptive information and if the AI System is consider High Risk pursuant to in scope AI regulations.

Conduct Assessment

Conduct assessment using an AI risk management framework. Utilize assessment process to assess current state, gain alignment with organization stakeholders and determine future priorities.

Develop Roadmap

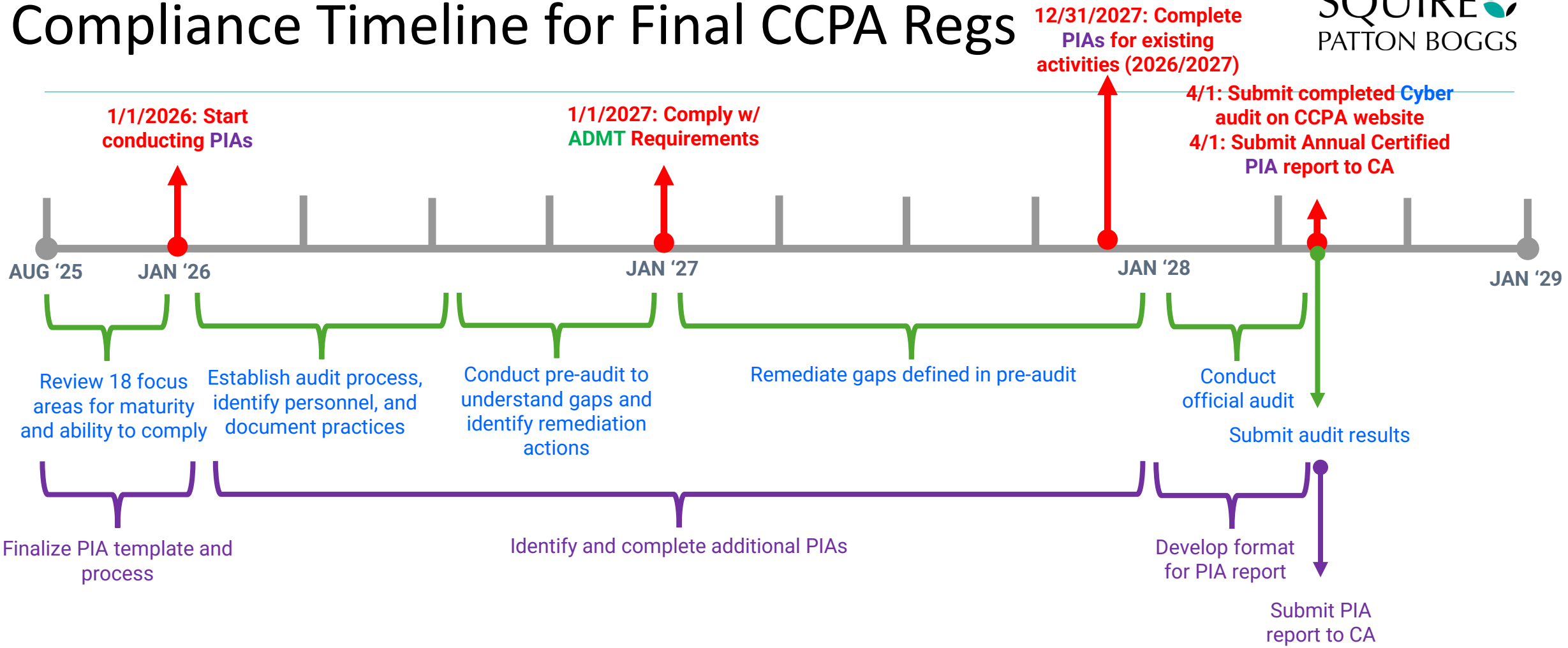
Using the output from the assessment, develop implementation roadmap to detail how toolkits will be operationalized. For example, certain aspects of client's existing program will be enhanced whereas in other cases the toolkit will be net new.

Operationalize Toolkits and Remediate Gaps

Operationalize toolkits or enhance existing artifacts to meet framework standards:

1. AI Risk Management Policy
2. Inventory of AI Systems *(complete)*
3. AI Impact Assessment Template
4. AI System Performance and Monitoring Template
5. AI System Risk Register
6. AI Incident Response Plan
7. Third Party Risk Management
8. AI Risk Management Training
9. Channels to receive AI updates

Compliance Timeline for Final CCPA Regs



KEY:
RED: Compliance deadlines per CCPA
BLUE: Recommended Cyber roadmap
PURPLE: Recommended PIA roadmap
GREEN: Recommended ADMT roadmap

Questions?

SPB Data Privacy Resources

SQUIRE PATTON BOGGS

Powered by SPB

Empower your data strategy with Squire Patton Boggs' comprehensive suite of privacy and cybersecurity tools — designed to help you navigate complex regulations and safeguard digital assets with confidence.

Privacy World Blog

Stay ahead of global data privacy trends with Privacy World Blog— your trusted source for expert analysis, legal updates, and practical guidance in an ever-evolving digital landscape.

Law & Policy Hub

Explore the future of law and technology at the Squire Patton Boggs AI Hub — your gateway to expert insights, legal innovation, and strategic guidance on artificial intelligence.

Appendix 1

State	Key Categories of Organizational Level Exemptions
California Law	• Providers of healthcare governed by the CMIA and covered entities under the HIPAA only to the extent the provider or covered entity maintains patient information in the same manner as medical information under the CMIA or protected health information under the HIPAA • Business associates of a covered entity governed by the HIPAA, only to the extent the business associate maintains, uses and discloses patient information in the same manner as medical information under the CMIA or protected health information under the HIPAA • Any nonprofit organization that do not fit the definition of "business"
Virginia Law	• Any body, authority, board, bureau, commission, district, or agency of the state or of any political subdivision of the state • Financial institutions subject to the GLBA • Covered entities or business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations, i.e., any corporation organized under the Virginia Nonstock Corporation Act (§ 13.1-801 et seq.), any political organizations, organizations exempt from taxation under the IRC that is identified under Va. Code Ann. § 52-41, and any subsidiary or affiliate of entities organized in pursuant to Chapter 9.1 of Title 56
Colorado Law	• Financial institutions or affiliates governed by the GLBA • National securities associations registered under the SEC Act • Air carriers, as defined in and regulated under 49 U.S.C. § 40101 and § 41713 ***Non-profits are <u>not</u> exempt***.
Utah Law	• Government entities or third parties acting on behalf of the government entities (as defined in the Utah Code § 63G-2-103) • Tribes • Financial institution or an affiliate of a financial institution governed by the GBLA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Non-profit corporations (defined in § 16-6a-102)

Appendix 1

Connecticut Law	• Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state and any person who has entered into a contract with any body, authority, board, bureau, commission, district or agency while such person is processing consumer health data on behalf of such body, authority, board, bureau, commission, district or agency pursuant to such contract. • Financial institutions subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the IRC • National securities associations registered under the SEC Act • Nonprofit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the IRC • National securities associations registered under the SEC Act
Iowa Law	• State or any political subdivision of the state • Financial institutions or affiliates of financial institutions subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(6), or 501(c)(12) of the IRC, or state law and any organization exempt from taxation under Section 501(c)(4) of the IRC that is established to detect or prevent insurance-related crime or fraud ***Most non-profits are not exempt.***
Indiana Law	• State agency, or a body, authority, board, bureau, commission, district, or agency of any political subdivision of the state • A third party under contract with a state or local government entity, when acting on behalf of the entity • Financial institutions or affiliates subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(6), or 501(c)(12) of the IRC • Public utilities (as defined in IC 8-1-2-1(a)) or service company affiliated with a public utility

Appendix 1

Tennessee Law	• A body, authority, board, bureau, commission, district, or agency of the state or of a political subdivision of the state • Financial institutions or affiliates subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations meaning a corporation organized under the Tennessee Nonprofit Corporation Act, an organization exempt from taxation under the IRC, a public utility organized under the laws of the state, or an entity owned or controlled by a nonprofit organization • Individuals, firms, associations, corporations, or entities licensed in Tennessee as insurance companies • Consumer reporting agency or furnisher that provides information for use in a consumer report, and a user of a consumer report, but only to the extent that the activity/ processing of the information is regulated under the FCRA
Montana Law	• Body, authority, board, bureau, commission, district, or agency of this state or any political subdivision of the state • Financial institutions or affiliates subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Non-profit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the IRC • National securities associations registered under the SEC Act
Florida Law	• State agency or political subdivision • Financial institutions subject to the GLBA • Covered entities and business associates subject to the HIPAA • Postsecondary education institutions • Nonprofit organizations that are exempt from taxation under the IRC or a political organization

Appendix 1

Texas Law	• State agency or a political subdivision of the state • Financial institution subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations, i.e., a corporation organized under the Texas Business Organizations Code Chapters 20 and 22, and the provisions of Title 1, to the extent applicable to nonprofit corporations, a political organization, organizations exempt from taxation under the IRC (including § 501(c)(19)) and organizations exempt from taxation under the IRC § 501(c)(4) that is identified under TX Insurance Code § 701.052 (a) • Electric utilities, power generation companies, or a retail electric providers as defined by the Utilities Code § 31.002

Oregon Law	• Public corporations, including the Oregon Health and Science University and the Oregon State Bar, or a public body (as defined in ORS 174.109)
	• Nonprofit organizations established to detect and prevent fraudulent acts in connection with insurance
	• Non-commercial activities of:
	  ○ A publisher, editor, reporter or other person who is connected with or employed by a newspaper, magazine, periodical, newsletter, pamphlet, report or other publication in general circulation
	  ○ A radio or television station that holds a license issued by the Federal Communications Commission
	  ○ A nonprofit organization that provides programming to radio or television networks
	  ○ An entity that provides an information service, including a press association or wire service
	• Insurers, as defined in ORS 731.106
	• Insurance Producers, as defined in ORS 731.104
	• Insurance consultants, as defined in ORD 744.602
	• Consumer reporting agencies, as defined in the FCRA
	• A furnisher, as defined in the FCRA
	• A person who uses a consumer report under the FCRA (15 U.S.C. § 1681b(a)(3).)
	• Financial Institutions, as defined in ORD 706.008, or affiliates or subsidiary that is only and directly engaged in financial activities, as defined in 12 U.S.C. § 1843(k)
	• Persons holding a third-party administrator license issued under ORS 744.710
	
	Most nonprofits are <u>not</u> exempt.

Appendix 1

Delaware Law	• Any regulatory, administrative, advisory, executive, appointive, legislative, or judicial body of the state or a political subdivision of the state, including any board, bureau, commission, agency of the state or a political subdivision of the state, (excluding any institution of higher education) • Financial institutions or affiliates subject to the GLBA • Nonprofit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the IRC, that are *dedicated exclusively* to preventing and addressing insurance crime • National securities associations registered under the SEC Act • Registered futures associations pursuant to the Commodity Exchange Act ***Most non-profits are <u>not</u> exempt***.
New Jersey Law	• Any state agency, any political subdivision, and any division, board, bureau, office, commission, or other instrumentality created by a political subdivision • Financial institutions and affiliates subject to the GLBA • Insurance institutions subject to P.L.1985, c.179 (C.17:23A-1 et seq.) • Secondary market institutions identified in 15 U.S.C. § 6809(3)(D) and 12 C.F.R. § 1016.3(l)(3)(iii) ***Non-profits are <u>not</u> exempt***.
New Hampshire Law	• Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of the state • Financial institutions subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the IRC • National securities associations registered under the SEC Act

Appendix 1

Kentucky Law	• City, state agency, or any political subdivision of the state • Financial institutions or affiliates subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institution of higher education • Nonprofit organizations under Section 501(c)(3) of the IRC and corresponding state law, i.e., any incorporated or unincorporated entity that is operating for religious, charitable, or educational purposes, and does not provide earnings to, or operate in any manner that inures to the benefit of, any officer, employee, or shareholder of the entity. • Organizations that do not provide net earnings to any officer, employee, or shareholder of the entity, and is recognized under KRS 304.47-060(1)(e) as assisting law enforcements agencies with suspected insurance-related criminal or fraudulent acts or first responders with catastrophic events • Small telephone utility as defined in KRS 278.516, a Tier III CMRS provider as defined in KRS 65.7621, or a municipally owned utility that does not sell or share personal data with any third-party processor
Maryland Law	• A regulatory, administrative, advisory, executive, appointive, legislative, or judicial body or instrumentality of the state, including a board, bureau, commission, or unit of the state or a political subdivision of the state • Financial institutions or affiliates subject to the GLBA • A nonprofit controller that process or shares personal data solely for the purposes of assisting law enforcement agencies investigating criminal or fraudulent acts relating to insurance or first responders during catastrophic events • National securities associations registered under the SEC Act ***Most non-profits are <u>not</u> exempt.***
Nebraska Law	• State agency or political subdivision of the state • Financial institutions or affiliates subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Non-profit organizations meaning any corporation organized under the Nebraska Nonprofit Corporation Act, any organization exempt from taxation under Section 501(c)(3), 501(c)(6), or 501(c)(12) of the IRC, any organization exempt from taxation under Section 501(c)(4) of the IRC that is established to detect or prevent insurance-related crime or fraud, and any subsidiary or affiliate of a cooperative corporation organized in Nebraska • Electricity suppliers (as defined in NE Code 70-1001.01) • Natural gas public utilities (as defined in NE Code 66-1802) • Municipal natural gas utilities

Appendix 1

Rhode Island Law	• Any body, authority, board, bureau, commission, district or agency of the state or any political subdivision of the state (including specifically a contractor, subcontractor, or agent of a state agency or local unit of government when working for that state agency or local unit of government) • Financial institutions subject to the GLBA • Covered entities and business associates subject to the HIPAA • Institutions of higher education • Nonprofit organizations that are exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the IRC • National securities association that is registered under 15 U.S.C. § 78o-3 of the SEC Act
Minnesota Law	• Government entity, which means a state agency, statewide system, or political subdivision (Minn. Stat. § 13.02(7)(a).) • Federally recognized Indian tribe • State or federally chartered bank or credit union, or an affiliate or subsidiary • Nonprofit organization *established to detect and prevent fraudulent acts in connection with insurance* • A small business, as defined by the SBA • Insurance company, as defined in § 60A.02, subdivision 4, an insurance producer, as defined in § 60K.31, subdivision 6, a third-party administrator of self-insurance, or an affiliate or subsidiary of any entity identified in this clause that is principally engaged in financial activities, as described in 12 U.S.C. § 1843(k), except that this clause does not apply to a person that, alone or in combination with another person, establishes and maintains a self-insurance program that does not otherwise engage in the business of entering into policies of insurance • An air carrier subject to the Airline Deregulation Act *only to the extent* that the air carrier collects personal data related to prices, routes, or services and only to the extent that the provisions of the Airline Deregulation Act preempt the requirements of MN-DPA. ***Most non-profits are <u>not</u> exempt***.

Appendix 1

Data Level Exemptions

The state consumer privacy laws generally exempt personal data processed in the context of a purely personal or household activity.

State	Exempt Data Level Exemptions
California Law	· Aggregate consumer information (§ 1798.140(b).) · De-identified information (§ 1798.140(m).) · Publicly available information (§ 1798.140(v)(2).) · Personal information collected, processed, sold, or disclosed subject to the GLBA. This exemption does not apply to § 1798.150, which relates to personal information security breaches · Protected health information collected by a covered entity or business associate under the HIPAA · Medical information governed by the CMIA · Personal information collected as part of a clinical trial or other biomedical research study subject to or conducted in accordance with the Common Rule, provided that the information is not sold or shared in a manner not permitted by the Common Rule, and, if it is inconsistent, that participants are informed of that use and provide consent · Information It is deidentified in accordance with the requirements for deidentification set forth in 45 CFR 164.514 and is derived from patient information that was originally collected, created, transmitted or maintained by an entity regulated by the HIPAA, the CMIA or the Common Rule · Collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency and by a user of a consumer report to the extent that the activity is subject to regulation under the FCRA and the information is not collected, maintained, used, communicated, disclosed or sold except as authorized by the FCRA. This exemption does not apply to § 1798.150, which relates to personal information security breaches · § 1798.105 (right to delete) and § 1798.120 (right to opt out of sale or sharing) do not apply to a commercial credit reporting agency's collection, processing, sale or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns, or contact the consumer only in the consumer's role as the owner, director, officer or management employee of the business · Personal information collected, processed, sold, or disclosed subject to the California Financial Information Privacy Act. This exemption does not apply to § 1798.150, which relates to personal information security breaches) · Personal information collected, processed, sold, or disclosed subject to the Farm Credit Act. This exemption does not apply to § 1798.150, which relates to personal information security breaches · Personal information collected, processed, sold or disclosed subject to the DPPA. This exemption does not apply to § 1798.150, which relates to personal information security breaches · § 1798.120 (right to opt out of sale or sharing) does not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle manufacturer, if the vehicle information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall pursuant to 49 U.S.C. § 30118-30120, provided that the new motor vehicle dealer or vehicle manufacturer does not sell, share or use that information for any other purpose · § 1798.120 (right to opt out of sale or sharing) does not apply to vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, if the information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall conducted pursuant to 46 U.S.C. § 4310, provided that the dealer or vessel manufacturer does not sell, share or use the information for any other purpose · Obligations under § 1798.105 (right to delete), § 1798.106 (right to correct), § 1798.110 (right to know and access), and § 1798.115 (right to know what personal information to sold or shared and to whom) do not apply to household data

Appendix 1

Virginia Law	· De-identified data (§ 59.1-575.) · Publicly available information (§ 59.1-575.) · Data subject to the GLBA · Protected health information under the HIPAA, and information derived · Information used for public health activities as authorized by the HIPAA · Health records for purposes of Title 32.1 · Patient identifying information for purposes of 42 U.S.C. § 290dd-2 · Identifiable private information processed for purposes of the Common Rule · Patient safety work product for purposes of the Patient Safety and Quality Improvement Act · Information and documents created for the Health Care Quality Improvement Act · Personal information regulated under the FCRA · Personal data subject to the DPPA · Personal data regulated by the Farm Credit Act · Personal data subject to the FERPA · Data processed in the context of an employment or independent contractor/agent relationship · Data processed for employment emergency contact purposes · Data processed to administer employment benefits
Colorado Law	· De-identified data (§ 6-1-1303(11).) · Publicly available information (§ 6-1-1303(17)(b).) · Personal data governed by the GLBA · Protected health information under the HIPAA · Information and documents created by a covered entity for purposes of complying with the HIPAA · Healthcare information governed by Colorado's Title 25, Art. 1, Part 8 · Personal data governed by the Colorado Health Benefit Exchange Act · Patient identifying information, as defined in 42 CFR 2.11, that is governed by and collected and processed pursuant to 42 CFR 2, established pursuant to 42 U.S.C. § 290dd-2 · Identifiable private information processed for purposes of the Common Rule · Identifiable private information collected as part of human subjects research · Patient safety work product for purposes of the Patient Safety and Quality Improvement Act · Personal information bearing on a consumer's credit by a consumer reporting agency or related entities under the FCRA · Personal data governed by the DPPA · Personal data governed by the FERPA · Personal data governed by the COPPA · Data maintained for employment records · Customer data maintained by a public utility as defined in § 40-1-103(1)(a)(i) or an authority as defined in § 43-4-503(1), if the data is not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law · Data maintained by a state institution of higher education, the judicial department, or a county, city, or municipality

Appendix 1

Utah Law	· Aggregated data (§ 13-61-101(3).) · De-identified data (§ 13-61-101(14).) · Publicly available information (§ 13-61-101(14).) · Data subject to the GLBA · Protected health information under the HIPAA, and information derived · Patient identifying information for purposes of 42 C.F.R. Part 2 · Information and documents created specifically for, collected and maintained by a committee in § 26-1-7 · Identifiable private information processed for purposes of the Common Rule · Patient safety work product for purposes of the Patient Safety and Quality Improvement Act · Information and documents created for the Health Care Quality Improvement Act · Information regulated under the FCRA · Personal data subject to the DPPA · Personal data regulated by the Farm Credit Act · Personal data subject to the FERPA · Data processed in the context of an employment or independent contractor/agent relationship · Data processed for employment emergency contact purposes · Data processed to administer employment benefits
Connecticut Law	· De-identified data (§ 42-515(13).) · Publicly available information (§ 42-515(25).) · Data subject to the GLBA · Protected health information under the HIPAA, and information derived from such information · Information used for public health activities and purposes as authorized by the HIPAA · Patient-identifying information for purposes of 42 USC § 290dd-2 · Identifiable private information processed for purposes of the Common Rule · Data related to the protection of human subjects · Patient safety work product for purposes of the Patient Safety and Quality Improvement Act · Information and documents created for purposes of the Health Care Quality Improvement Act · Information bearing on creditworthiness regulated by the FCRA · Personal data regulated by the DPPA · Personal data regulated by the Farm Credit Act · Personal data regulated by the FERPA · Data maintained for employment records · Data processed for employment emergency contact purposes · Data processed to administer employment benefits · Personal data regulated by the Airline Deregulation Act

Appendix 1

Iowa Law	• Aggregate data (§ 715D.1(2).) • De-identified data (§ 715D.1(10).) • Publicly available information (§ 715D.1(24).) • Data subject to the GLBA • Protected health information under the HIPAA, and information derived • Information used only for public health activities, as authorized by the HIPAA • Health records • Patient identifying information for purposes of 42 USC § 290dd-2 • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created under the Health Care Quality Improvement Act • Information subject to the FCRA • Personal data regulated by the DPPA • Personal data regulated by the Farm Credit Act • Personal data regulated by the FERPA • Personal data used in accordance with the COPPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits
Indiana Law	• Aggregate data (§ 24-15-2-2.) • De-identified data (§ 24-15-2-12.) • Publicly available information (§ 24-15-2-26.) • Data subject to the GLBA • Protected health information under the HIPAA, and information derived • Information used for public health activities, as authorized by the HIPAA • Patient identifying information for purposes of 42 USC § 290dd-2 • Personal information collected as part of a clinical trial or research subject to the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information created for the Health Care Improvement Act • Personal data regulated by the FCRA • Personal data regulated by the DPPA • Personal data regulated by the Farm Credit Act • Personal data regulated by the FERPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits

Appendix 1

Tennessee Law	• Aggregated data (not defined) • De-identified data (§ 47-18-3201(11).) • Publicly available information • Data subject to the GLBA • Protected health information under the HIPAA, and information derived • Information used for public health activities as authorized by the HIPAA • Information included in a limited data set under the Privacy Rule (45 C.F.R. § 164.514(e).) • Patient identifying information for purposes of 42 U.S.C. § 290dd-2 • Health records for purposes of title 68 • Identifiable private information processed for purposes of the Common Rule • Information collected as part of public or peer-reviewed scientific or statistical research in the public interest • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for the Health Care Quality Improvement Act • Personal information used in a consumer report (i.e., bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living) and a user of a consumer report but only to the extent that the processing of the information is regulated under the FCRA • Consumer reporting agency or furnisher that provides information for use in a consumer report, and a user of a consumer report but only to the extent that the collection, maintenance, disclosure, sale, communication, or use of personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a is regulated by the FCRA • Personal information regulated under the DPPA • Personal information regulated by the Farm Credit Act • Personal information regulated by the FERPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits
Montana Law	• De-identified data (§ 30-14-2802(11).) • Publicly available information (§ 30-14-2802(22).) • Personal data subject to the GLBA • Protected health information under the HIPAA, and information derived from such information • Information used for public health activities as authorized by the HIPAA • Patient identifying information for purposes of 42 USC § 290dd-2 • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for the Health Care Quality Improvement Act • Personal information regulated by the FCRA • Personal data regulated by the DPPA • Personal data regulated by the Farm Credit Act

Appendix 1

Montana Law	• Personal data regulated by the FERPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits • Personal data subject to the Airline Deregulation Act
Florida Law	• De-identified data (§ 501.702 (13).) • Publicly available information (§ 501.702 (28).) • Data subject to the GLBA • Protected health information under the HIPAA • Information used for public health activities authorized by the HIPAA • Health records • Patient identifying information for purposes of 42 USC § 290dd-2 • Identifiable private information processed for purposes of the Common Rule • Identifiable private information collected as part of human subjects' research • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for purposes of the Health Care Quality Improvement Act • Information derived from any of the health-care related information above • Personal data used in activities regulated by the FCRA • Personal data regulated by the DPPA • Personal data regulated by the Farm Credit Act • Personal data regulated by the FERPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits • Personal data subject to the Airline Deregulation Act

Appendix 1

Florida Law	• Personal data collected and transmitted which is necessary for the sole purpose of sharing such personal data with a financial service provider solely to facilitate short term, transactional payment processing for the purchase of products or services • Personal data shared between a manufacturer of a tangible product and authorized third-party distributors or vendors of the product, as long as such personal data is used solely for advertising, marketing, or servicing the product that is acquired directly through such manufacturer and such authorized third-party distributors or vendors
Texas Law	• De-identified data (§ 541.001(12).) • Publicly available information (§ 541.001(12).) • Data subject to the GLBA • Protected health information under the HIPAA, and information derived • Information collected or used only for public health activities and purposes as authorized by the HIPAA • Health records • Information included in a limited data set under The Privacy Rule (45 C.F.R. § 164.514(e).) • Information subject to Controlled Substances Act for purposes of compliance with listed chemicals • Patient identifying information for purposes of 42 U.S.C. § 290dd-2 • Identifiable private information processed for purposes of the Common Rule • Information collected as part of a public or peer reviewed scientific or statistical research in the public interest • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for the Health Care Quality Improvement Act • Personal information regulated under the FCRA • Personal data subject to the DPPA • Personal data regulated by the Farm Credit Act • Personal data subject to the FERPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed and is necessary to administer employment benefits to beneficiaries/dependents

Appendix 1

Oregon Law	• De-identified data (§ 646A.570(11).) • Data that is lawfully available through federal, state, or local government records or widely distributed media or that a controller reasonably has understood to have been lawfully made available to the public by a consumer (§ 646A.570(13)(b).) • Information collected, processed, sold or disclosed subject to the GLBA • Protected health information under the HIPAA • Patient-identifying information, as defined in in 42 C.F.R. 2.11, as in effect on January 1, 2024, that is collected and processed in accordance with 42 C.F.R. part 2 • Information used for public health activities and purposes described in 45 C.F.R. 164.512 • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information created for purposes of the Health Care Quality Improvement Act • Information subject to the FCRA • Information subject to the DPPA • Information subject to the FERPA • Personal data processed in the context of an employment or application for employment • Personal data processed regarding an individual's contractual relationship with a business entity • Personal data processed regarding an individual's ownership or function as a director or officer of a business entity • Personal data processed to administer employee benefits (including benefits for the individual's dependents or beneficiaries) • Personal data processed for emergency contact purposes • Data subject to the Airlines Deregulation Act • Non-commercial activity related to media programming and publication, radio/television, and information services
Delaware Law	• De-identified data (§ 12D-102(14).) • Publicly available information (§ 12D-102(28).) • Data subject to the GLBA • Protected health information under the HIPAA • Information to the extent it is used for public health activities as authorized by the HIPAA • Patient-identifying information for purposes of 42 USC § 290dd-2 • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information subject to the FCRA • Personal data subject to the DPPA • Personal data subject to the Farm Credit Act • Personal data regulated by the FERPA

Appendix 1

Delaware Law	• Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits • Personal data subject to the Airline Deregulation Act • Information of a victim or witness to abuse maintained by a nonprofit organization providing services to victims of abuse
New Jersey Law	• De-identified data (§ 56:8-166.4.) • Publicly available information (§ 56:8-166.4.) • Data regulated by the GLBA • Protected health information collected by a covered entity or business associate subject to the privacy, security, and breach notification rules under the HIPAA • Identifiable private information processed for purposes of the Common Rule • Personal data processed pursuant to the FCRA • The sale of a consumer's personal data by the New Jersey Motor Vehicle Commission that is permitted by the DPPA
New Hampshire Law	• De-identified data (§ 507-H:1(XIV).) • Publicly available information (§ 507-H:1(XXVI).) • Data subject to the GLBA • Protected health information defined under the HIPAA, and information derived from information that is de-identified in accordance with the requirements for de-identification pursuant to the HIPAA • Information used for public health activities as authorized by the HIPAA • Patient identifying information for purposes of 42 USC § 290dd-2 • Information included in a limited data set as described and used under the Privacy Rule (45 C.F.R. § 164.514(e).) • Data maintained or used for purposes of compliance to the Controlled Substances Act 21 U.S.C. § 830 • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information subject to the Health Care Quality Improvement Act • Personal information processed pursuant to the FCRA • Personal data processed pursuant to the DPPA • Personal data processed pursuant to the Farm Credit Act • Personal data regulated by the FERPA • Data processed in the context of an employment or independent contractor/agent relationship

Appendix 1

New Hampshire Law	• Data processed for employment emergency contact purposes • Data processed to administer employment benefits • Personal data processed pursuant to the Airline Deregulation Act
Kentucky Law	• De-identified data (§ 367.3611(11).) • Publicly available information (§ 367.3611(26).) • Data subject to Title V of the GLBA • Protected health information defined under the HIPAA • Information used only for public health activities and purposes as authorized by the HIPAA • Information derived from information that is deidentified in accordance with the requirements for deidentification under the HIPAA • Health records • Patient identifying information for purposes of 42 C.F.R. § 2.11 • Identifiable private information processed for purposes of the Common Rule • Personal information collected as part of a clinical trial or study subject to the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Personal information and documents created under the Health Care Quality Improvement Act • Data processed pursuant to the FCRA • Personal data processed pursuant to the DPPA • Personal data regulated by the Farm Credit Act • Personal data processed pursuant to the FERPA • Personal data used in accordance with the COPPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits • Data processed by a utility as defined in KRS 278.010 • Data processed under the Combat Methamphetamine Epidemic Act of 2005 (Title VII)

Appendix 1

Maryland Law	• De-identified data (§ 14–4601(P).) • Publicly available information (§ 14–4601(CC).) • Data that is subject to Title V of the GLBA • Protected health information under the HIPAA, • Information deidentified according to the HIPAA • Information used for public health community health, or population health activities and purposes as authorized by the HIPAA when provided by or to a covered entity or when provided by or to a business associate in accordance with the business associate agreement with a covered entity • Patient identifying information for purposes of 42 USC § 290dd-2 • Identifiable private information processed for purposes of the Common Rule • Personal information collected as part of a clinical trial or study subject to the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for the Health Care Quality Improvement Act • Personal information processed pursuant to the FCRA • Personal data processed pursuant to the DPPA • Personal data regulated by the Farm Credit Act • Personal data regulated by the FERPA • Personal data used in accordance with the COPPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits • Personal data subject to the Airline Deregulation Act • Data collected by or on behalf of a person regulated under the insurance article or an affiliate of such a person, in furtherance of the business of insurance
Nebraska Law	• De-identified data (§ 87-1102(12).) • Publicly available information (§ 87-1102(28).) • Data subject to Title V of the GBLA • Protected health information under the HIPAA • Information derived from information that is deidentified in accordance with the requirements for deidentification under the HIPAA • Information used for public health activities and purposes as authorized by the HIPAA • Health records • Patient identifying information for purposes of 42 USC 290dd-2 • Identifiable private information processed for purposes of the Common Rule

Appendix 1

Minnesota Law	• Publicly available information (§ 325O.02(p).) • Personal data collected, processed, sold, or disclosed pursuant to the GLBA • Information that originated from, or intermingled with, information regulated by the GLBA and that a licensed residential mortgage originator, as defined under § 58.02, subdivision 19, or residential mortgage servicer, as defined under § 58.02, subdivision 20, collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified by the GLBA • Protected health information defined under the HIPAA • Information deidentified according to the HIPAA • Health records, as defined in § 144.291, subdivision 2 • Patient identifying information for purposes of the 42 CFR part 2, established pursuant to 42 USC § 290dd-2 • Information derived from patient information that was originally collected, created, transmitted or maintained by an entity regulated by the HIPAA, a health care provider, as defined in § 144.291, subdivision 2, or a program or a qualified service organization, as defined by the Confidentiality of Substance Use Disorder Regulations • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for purposes of the Health Care Quality Improvement Act and related regulations • Information used only for public health activities and purposes, as described under 45 CFR § 164.512 • Personal data processed pursuant to the FCRA, only when the activity, use, or entity is subject to the FCRA • Information that originates from, or is intermingled so as to be indistinguishable from, information subject to the FCRA and that a person licensed under Chapter 56 collects, processes, uses, or maintains in the same manner as is required under the laws and regulations subject to the FCRA • Personal data collected, processed, sold, or disclosed pursuant to the DPPA • Personal data collected, processed, sold, or disclosed pursuant to the Farm Credit Act • Personal data regulated by the FERPA • Data collected or maintained in the course of an individual acting as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of a business if the data is collected and used solely within the context of the role • Data collected or maintained as the emergency contact information of an individual for employment emergency contact purposes • Data collected or maintained that is necessary for the business to retain to administer employment benefits for another individual relating to the individual if used solely for the purposes of administering those benefits • Personal data collected, processed, sold, or disclosed pursuant to the Minnesota Insurance Fair Information Reporting Act in § 72A.49 to 72A.505 • Data collected, processed, sold, or disclosed as part of a payment-only credit, check, or cash transaction where no data about consumers, are retained

Appendix 1

Nebraska Law	• Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for the Health Care Quality Improvement Act • Personal information regulated by the FCRA • Personal data regulated by the DPPA • Personal data regulated by the Farm Credit Act • Personal data regulated by the FERPA • Data processed in the context of an employment or independent contractor/agent relationship • Data processed for employment emergency contact purposes • Data processed to administer employment benefits
Rhode Island Law	• De-identified data (§ 6-48.1-2(13).) • Publicly available information (§ 6-48.1-2(24).) • Data subject to the GLBA • Protected health information under the HIPAA and information derived from it • Information used for public health activities as authorized by the HIPAA • Patient-identifying information for purposes of 42 U.S.C. § 290dd-2 • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for the Health Care Quality Improvement Act • Personal information regulated by the FCRA • Personal data processed in compliance with the DPPA • Personal data processed in compliance with the Farm Credit Act • Personal data regulated by the FERPA • Data processed in the context of an employment or independent contractor/agent relationship with a controller, processor or third party • Data processed for employment emergency contact purposes • Data processed to administer employment benefits • Personal data regulated by the Airline Deregulation Act

Appendix 1

Minnesota Law	Publicly available information (§ 325O.02(p).) • Personal data collected, processed, sold, or disclosed pursuant to the GLBA • Information that originated from, or intermingled with, information regulated by the GLBA and that a licensed residential mortgage originator, as defined under § 58.02, subdivision 19, or residential mortgage servicer, as defined under § 58.02, subdivision 20, collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified by the GLBA • Protected health information defined under the HIPAA • Information deidentified according to the HIPAA • Health records, as defined in § 144.291, subdivision 2 • Patient identifying information for purposes of the 42 CFR part 2, established pursuant to 42 USC § 290dd-2 • Information derived from patient information that was originally collected, created, transmitted or maintained by an entity regulated by the HIPAA, a health care provider, as defined in § 144.291, subdivision 2, or a program or a qualified service organization, as defined by the Confidentiality of Substance Use Disorder Regulations • Identifiable private information processed for purposes of the Common Rule • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act • Information and documents created for purposes of the Health Care Quality Improvement Act and related regulations • Information used only for public health activities and purposes, as described under 45 CFR § 164.512 • Personal data processed pursuant to the FCRA, only when the activity, use, or entity is subject to the FCRA • Information that originates from, or is intermingled so as to be indistinguishable from, information subject to the FCRA and that a person licensed under Chapter 56 collects, processes, uses, or maintains in the same manner as is required under the laws and regulations subject to the FCRA • Personal data collected, processed, sold, or disclosed pursuant to the DPPA • Personal data collected, processed, sold, or disclosed pursuant to the Farm Credit Act • Personal data regulated by the FERPA • Data collected or maintained in the course of an individual acting as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of a business if the data is collected and used solely within the context of the role • Data collected or maintained as the emergency contact information of an individual for employment emergency contact purposes • Data collected or maintained that is necessary for the business to retain to administer employment benefits for another individual relating to the individual if used solely for the purposes of administering those benefits • Personal data collected, processed, sold, or disclosed pursuant to the Minnesota Insurance Fair Information Reporting Act in § 72A.49 to 72A.505 • Data collected, processed, sold, or disclosed as part of a payment-only credit, check, or cash transaction where no data about consumers, are retained

Appendix 2

Consumer Rights and Business Obligations: Comparative Chart

The following chart demonstrates the similarities and differences among current state consumer privacy laws of general application, compares them to the GDPR and notes differences between the original CCPA and the current version amended by CPRA.

Appendix 2

GDPR, CCPA, CPRA, Virginia Law & Colorado Law

	GDPR	CCPA	CPRA	Virginia Law	Colorado Law
Right to Access	✓	✓	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	Implied	Implied	✓	✓
Right to Data Portability	✓	✓	✓	✓	✓
Right to Delete[1]	✓	✓	✓	✓	✓
Right to Correct / Right to Rectification	✓	×	✓	✓	✓
Right to Opt-Out of Sale	✓[2]	✓[3]	✓[3]	✓[4]	✓[3]
Right to Opt-Out of Targeted / Behavioral Advertising[5]	✓	×[6]	✓	✓	✓
Right to Object or Opt-Out of ADM	✓	×	✓[7]	×	✓[8]
Right to Opt-Out of Profiling[9]	✓	×	✓	✓	✓
Choice Required for Processing of "Sensitive" Personal Data	Opt-In	×	Opt-Out[10]	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	✓	×	×	×	×
Required Opt-Out Links on Website or Elsewhere	No Explicit Requirement	DNS	DNSell, DNShare, Sensitive PI Opt-Out[11]	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs

Appendix 2

GDPR, CCPA, CPRA, Virginia Law & Colorado Law

	GDPR	CCPA	CPRA	Virginia Law	Colorado Law
Right to Non-Discrimination[12]	Implied	✓	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	Implied	✓	✓	✓
Privacy & Security Impact Assessments Sometimes Required	✓	x	✓	✓	✓
"Reasonable" Security Obligation	✓	Implied	✓	✓	✓
Notice at Collection Requirement	✓	✓ (Statute + Regs)	✓	x	x
Honor Universal Opt-out Signals	x	x	✓	x	✓

Appendix 2

Utah Law, Connecticut Law, Nevada Law, Iowa Law & Indiana Law

	Utah Law	Connecticut Law	Nevada Law	Iowa Law	Indiana Law[42]
Right to Access	✓	✓	×	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	×	✓	✓
Right to Data Portability	✓	✓	×	✓	✓
Right to Delete	✓	✓	×	✓	✓
Right to Correct / Right to Rectification	×	✓	×	×	✓
Right to Opt-Out of Sale	✓[34]	✓[33]	✓[43]	✓[34]	✓[34]
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	×	✓	✓
Right to Object or Opt-Out of ADM	×	×	×	×	×
Right to Opt-Out of Profiling	×	✓	×	×	✓
Choice Required for Processing of "Sensitive" Personal Data	Notice & Opp. to Opt-Out	Opt-In	×	Notice & Opp. to Opt-Out	Opt-In
Right to Object to or Restrict Processing Generally	×	×	×	×	×
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	None	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs
Right to Non-Discrimination	✓	✓	×	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	×	✓	×	×	✓
Privacy and Security Impact Assessments Sometimes Required	×	✓	×	×	✓
"Reasonable" Security Obligation	✓	✓	✓	✓	✓
Notice at Collection Requirement	×	×	×	×	×
Honor Universal Opt-out Signals	×	✓	×	×	×

Appendix 2

Tennessee Law, Montana Law, Florida Law, Texas Law & Oregon Law

	Tennessee Law	Montana Law	Florida Law[44]	Texas Law	Oregon Law[45]
Right to Access	✓	✓	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	✓	✓	✓
Right to Data Portability	✓	✓	✓	✓	✓
Right to Delete	✓	✓	✓	✓	✓
Right to Correct / Right to Rectification	✓	✓	✓	✓	✓
Right to Opt-Out of Sale	✓[34]	✓[33]	✓[33]	✓[33]	✓[33]
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	✓	✓	✓
Right to Object or Opt-Out of ADM	×	×	×	×	×
Right to Opt-Out of Profiling	✓	✓	✓	✓	✓
Choice Required for Processing of "Sensitive" Personal Data	Opt-In	Opt-In	Opt-In (with a right to opt out later)	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	×	×	×	×	×
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs
Right to Non-Discrimination	✓	✓	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	✓	✓	✓	✓
Privacy and Security Impact Assessments Sometimes Required	✓	✓	✓	✓	✓
"Reasonable" Security Obligation	✓	✓	✓	✓	✓
Notice at Collection Requirement	×	×	×	×	×
Honor Universal Opt-out Signals	×	✓	×	✓	✓

Appendix 2

Delaware Law, New Jersey Law, New Hampshire Law, Kentucky Law &

	Delaware Law[46]	New Jersey Law	New Hampshire Law	Kentucky Law	Minnesota Law[47]
Right to Access	✓	✓	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	✓	✓	✓
Right to Data Portability	✓	✓	✓	✓	✓
Right to Delete	✓	✓	✓	✓	✓
Right to Correct / Right to Rectification	✓	✓	✓	✓	✓
Right to Opt-Out of Sale	✓[33]	✓[33]	✓[33]	✓[34]	✓[33]
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	✓	✓	✓
Right to Object or Opt-Out of ADM	×	×	×	×	✓
Right to Opt-Out of Profiling	✓	✓	✓	✓	✓
Choice Required for Processing of "Sensitive" Personal Data	Opt-In	Opt-In	Opt-In	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	×	×	×	×	×
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad, Sale & Profiling Opt-Outs	Targeted Ad & Sale Opt-Outs	None	Not required but noted as an approved method.
Right to Non-Discrimination	✓	✓	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	✓	✓	✓	✓
Privacy and Security Impact Assessments Sometimes Required	✓	✓	✓	✓	✓
"Reasonable" Security Obligation	✓	✓	✓	✓	✓
Notice at Collection Requirement	×	×	×	×	×
Honor Universal Opt-out Signals	✓	✓	✓	×	✓

Maryland Law, Nebraska Law & Rhode Island Law

	Maryland Law[48]	Nebraska Law	Rhode Island Law
Right to Access	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	✓
Right to Data Portability	✓	✓	✓
Right to Delete	✓	✓	✓
Right to Correct / Right to Rectification	✓	✓	✓
Right to Opt-Out of Sale	✓[33]	✓[33]	✓[33]
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	✓
Right to Object or Opt-Out of ADM	×	×	×
Right to Opt-Out of Profiling	✓	✓	✓
Choice Required for Processing of "Sensitive" Personal Data	Only when strictly necessary, no sale allowed	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	×	×	×
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	×
Right to Non-Discrimination	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	✓	✓
Privacy and Security Impact Assessments Sometimes Required	✓	✓	✓
"Reasonable" Security Obligation	✓	✓	✓
Notice at Collection Requirement	×	×	×
Honor Universal Opt-out Signals	✓	✓	×

Appendix 2

[30] In California, Utah, and Iowa, deletion obligations are limited to PI collected from the consumer; all other state consumer privacy laws include PI collected about the consumer is in scope of the deletion right.

[31] Selling personal data under the GDPR generally would require the consent of the data subject for collection and would be subject to the right to object to processing.

[32] Any consideration sufficient, but cash consideration not required.

[33] Cash consideration required.

[34] Right to opt-out of cross-context behavioral advertising sharing for California; right to opt-out of targeted advertising in all other state consumer privacy laws.

[35] However, certain data disclosures inherent in this type of advertising are arguably a "sale," subject to opt-out rights. The CPRA Regulations combine the opt-out right for "sale" and "share."

[36] Subject to substantial expansion under the CPRA Regulations. Based on preliminary rulemaking activities, it appears that the CPPA is contemplating a GDPR-like approach for ADM and profiling.

[37] Under the CPA Rules, if a consumer requests to opt out of human involved automated processing, organizations can reject the request, but must inform the consumer of the rejection within 45 days and include the following information or link to such information: the decision subject to profiling, the categories of PI used, the logic used in the profiling process, the role of human involvement, how profiling is used in the decision-making process, benefits and potential consequences of the decision, and how consumers can correct or delete the data used in the profiling.

[38] The CPRA's concept of profiling is subject to change under the regulations. The profiling concepts in the other 2023 state consumer privacy laws require legal or substantially similar effects.

Appendix 2

[39] Under the CPRA, the Sensitive PI opt-out right applies to certain processing activities beyond business purposes. Section 7027 of the CA Regs includes contextual but not cross-context behavioral advertising.

[40] Businesses will be able to utilize "a single, clearly labeled link" to cover all opt-outs. The CA Regs permit titling the link "Your Privacy Choices" or "Your California Privacy Choices" plus an icon. It is not clear if organizations need to provide both sale/share and limit sensitive info opt-outs where it is not engaging in activities that necessitate both in order to use the alternative link. The former could work well to direct a consumer to the other state opt-outs too.

[41] The CCPA (and the CPRA) take a more onerous approach to non-discrimination with respect to financial incentives and price/service differences, requiring businesses to prove that they are reasonably related to the value of the consumer's data to the business.

[42] Indiana Law also provides the right to obtain a copy or a representative summary of the consumer's personal data provided to the controller.

[43] In Nevada, website and online service operators are required to offer an "opt-out," but only for limited disclosures of certain information and only if the disclosure is made in exchange for monetary consideration.

[44] Florida Law also contains the rights to: (i) opt out of the collection or processing of sensitive data; and (ii) opt out of the collection of personal data through voice or facial recognition.

[45] Oregon Law also contains the right to obtain a list of specific third parties to which the controller has disclosed the consumer's personal data, **OR** any personal data (at the controller's option).

Appendix 2

[46] Delaware Law also provides the right to obtain a list of categories of third-party recipients of the consumer's personal data, by category of personal data.

[47] Under the Minnesota Law, a consumer has a right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain the information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers' personal data may be provided instead

[48] Maryland Law also provides the right to obtain a list of the categories of third parties to which the controller has disclosed the consumer's personal data, **OR** a list of the categories of third parties to which the controller has disclosed any consumer's personal data IF the controller does not maintain this information in a format specific to the consumer.