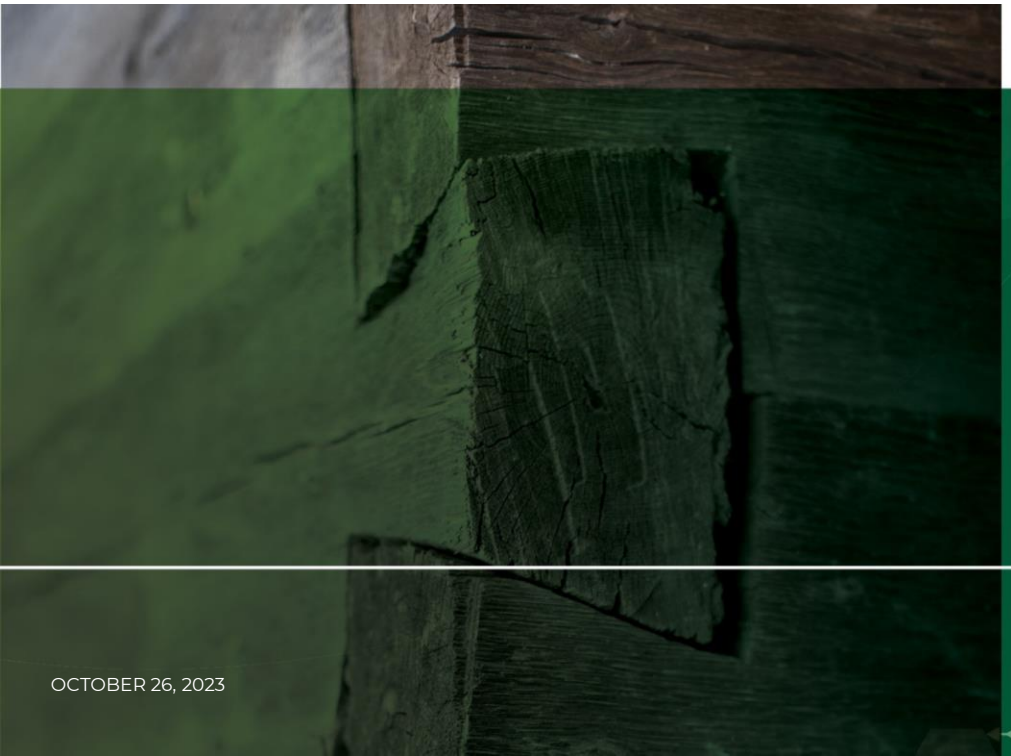
DOVETAIL
CONSULTING GROUP LLC

Privacy & Data Protection

CHANGES IN LAWS AND THE IMPACT ON OUR INDUSTRY



OCTOBER 26, 2023

Session

PANEL MEMBERS

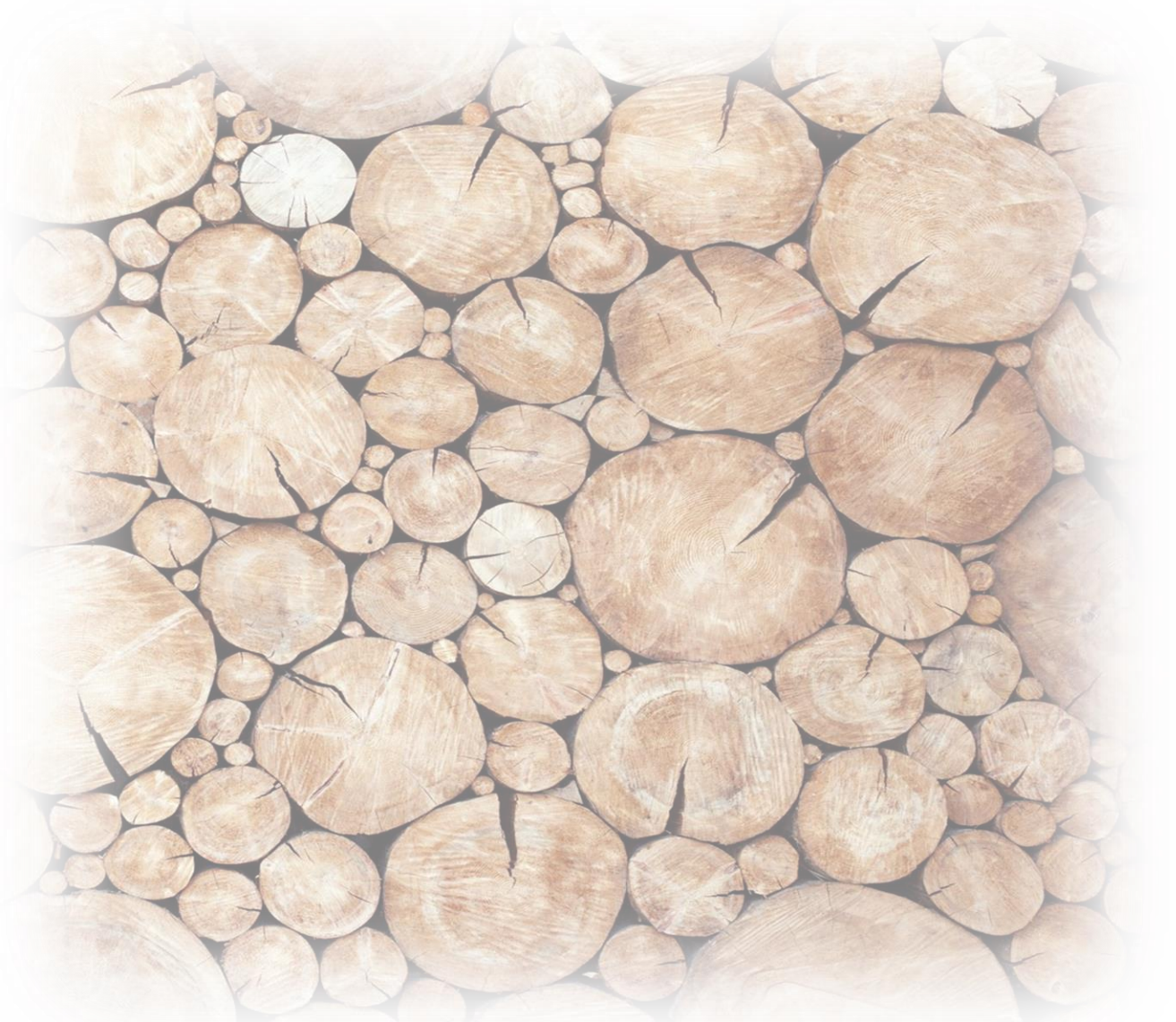
Katherine A. Chaurette
SVP, Healthcare Law & Compliance
Blueprint Medicines

Tiago Garrido
Chief Compliance Officer
Seres Therapeutics

Kris Hall (Moderator)
Managing Director
Dovetail Consulting Group

DOVETAIL
CONSULTING GROUP LLC

DISCUSSION AGENDA



1. **Privacy Landscape**
   Overview

2. **Panel Discussion**

3. **The Road Ahead**
   Preview

DOVETAIL
CONSULTING GROUP LLC

PRIVACY LANDSCAPE-*OVERVIEW*

DOVETAIL CONSULTING GROUP LLC

EXAMPLE - PRIVACY AND DATA PROTECTION LEGAL FRAMEWORKS

GDPR

European General Data Protection Regulation

- Applies to organizations offering goods/services to EU/EEA citizens
- Focus on individual rights
- Omnibus legislation, Implemented via Member States
- Penalties for non-compliance can reach 2%-4% annual revenue

CCPA / CPRA

California Consumer Privacy Act / Privacy Rights Act

- Applies to many organizations doing business in CA
- Focus on individual rights to control the collection / sale / sharing of information
- Imposes fines and provides private right of action for non-compliance

HIPAA

Health Insurance Portability & Accountability Act

- US Federal law - applies to "Covered Entities" (HCP/O, Insurance Cos, Pharmacies, etc. and their "Business Associates")
- Enforced by Office for Civil Rights and the Department of Justice (criminal)
- Privacy Rule
- Security Rule

CAN-SPAM

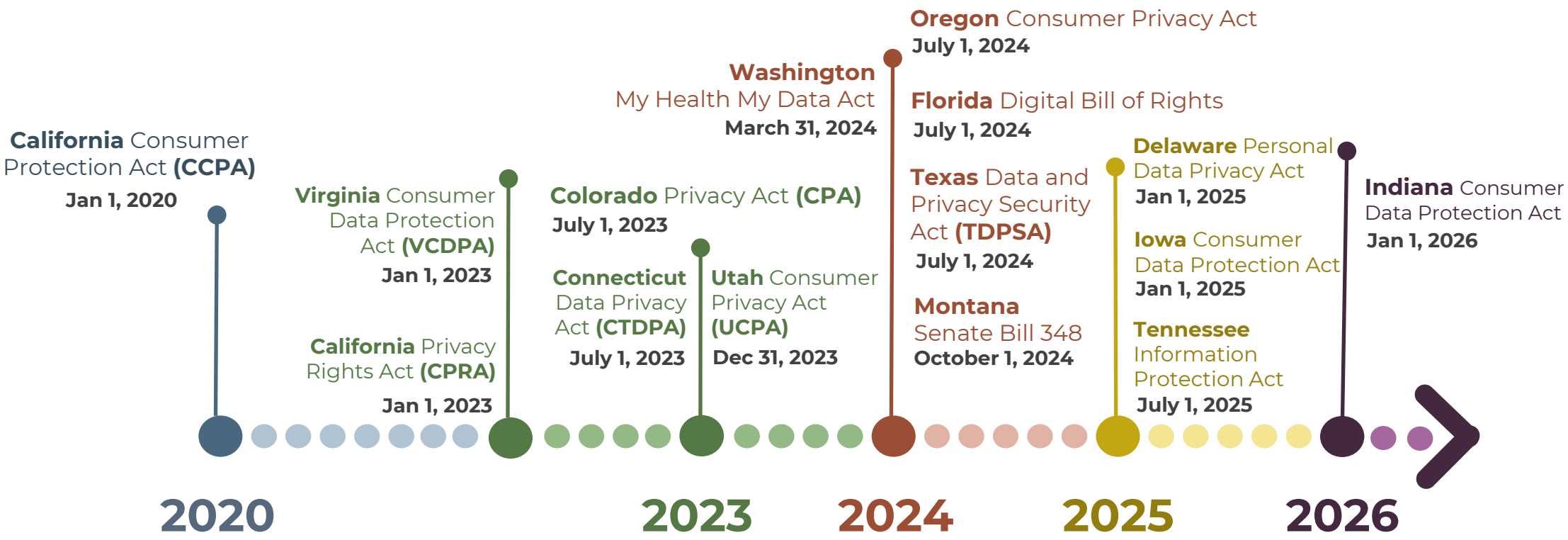
Controlling the Assault of Non-Solicited Pornography & Marketing Act

- US Federal law – applies to companies promoting products/services via electronic comms
- Provides right to opt out of unwanted emails
- Enforced by Federal Trade Commission; fines up to $42,530 per violation

DOVETAIL CONSULTING GROUP LLC

sample overview

U.S. STATE CONSUMER PRIVACY LAWS & EFFECTIVE DATES



DOVETAIL CONSULTING GROUP LLC

OBLIGATIONS

General overview of obligations imposed under recent U.S. State Privacy Laws

- ✓ **Notice/transparency requirement** — An obligation placed on a business to provide notice to consumers about certain data practices, privacy operations, and/or privacy programs and in some cases, obtain consent
- ✓ **Risk assessments** — An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects or procedures
- ✓ **Privacy Impact Assessments** – Requirement to assess and mitigate risks to individuals and their personal information on an activity basis
- ✓ **Opt-in default (requirement age)** — A restriction placed on a business to treat consumers under a certain age with an opt-in default for the sale of their personal information
- ✓ **Prohibition on discrimination (exercising rights)** — A prohibition against a business treating a consumer who exercises a consumer right differently than a consumer who does not exercise a right
- ✓ **Purpose/processing limitation** — An EU General Data Protection Regulation–style restrictive structure that prohibits the collection/processing of personal information except for a specific purpose

INDIVIDUAL RIGHTS

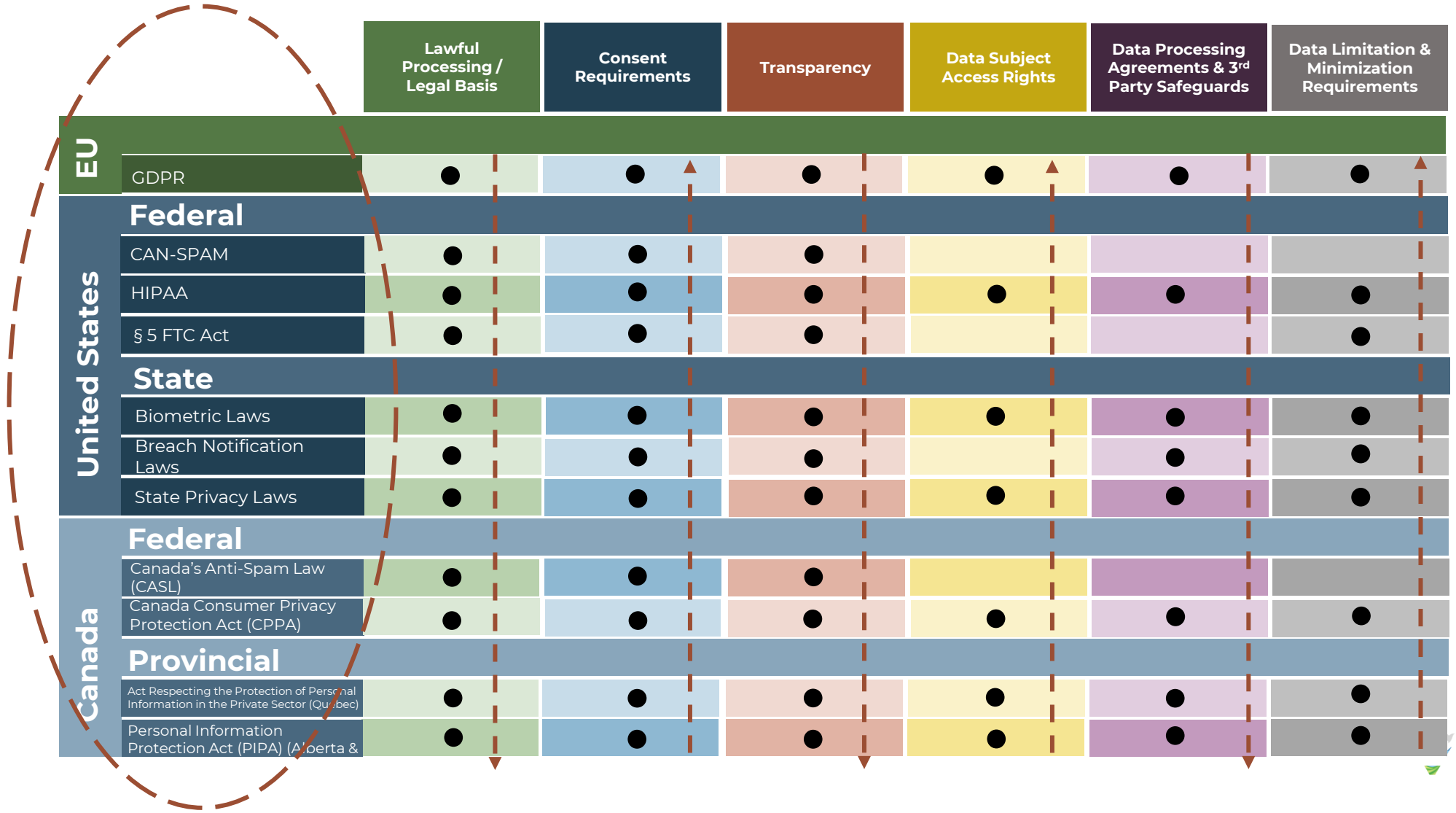
General overview of individual rights granted under recent U.S. State Privacy Laws

- ✓ **Right to access** — The right to access information or categories of information about:
  - Information collected
  - Information shared with third parties,
  - Specific third parties or categories of third parties to which the information was shared
- ✓ **Right to correct** — The right to request corrections to incorrect or outdated personal information
- ✓ **Right to delete** — The right to request deletion of personal information (barring certain exceptions)
- ✓ **Right to opt out of certain processing** — The right to restrict (for certain purposes) a business's processing of personal information.
- ✓ **Right to portability** — The right to request disclosure of personal information in a common file format
- ✓ **Right to opt-out of sales / sharing** — The right to prohibit the sale of personal information to third parties
- ✓ **Right to opt in for sensitive information processing** — The right to affirmatively consent to (opt in) the processing of sensitive personal information
- ✓ **Right against automated decision making** — A prohibition against decision-making based on an automated process without human input

DOVETAIL
CONSULTING GROUP LLC

sample overview

GLOBAL PRIVACY REQUIREMENTS



DOVETAIL
CONSULTING GROUP LLC

PART 2

PANEL DISCUSSION

DOVETAIL
CONSULTING GROUP LLC

Question 1

What are the most significant operational impacts you foresee (or have seen, thus far) because of the shifting US Privacy landscape?

DOVETAIL
CONSULTING GROUP LLC

Question 2

What are the most impactful steps you have taken as an organization thus far to address these changes?

DOVETAIL
CONSULTING GROUP LLC

Question 3

What do you think are the biggest challenges to implementing an effective Privacy Program to address the evolving data protection environment?

DOVETAIL
CONSULTING GROUP LLC

COMING SOON!

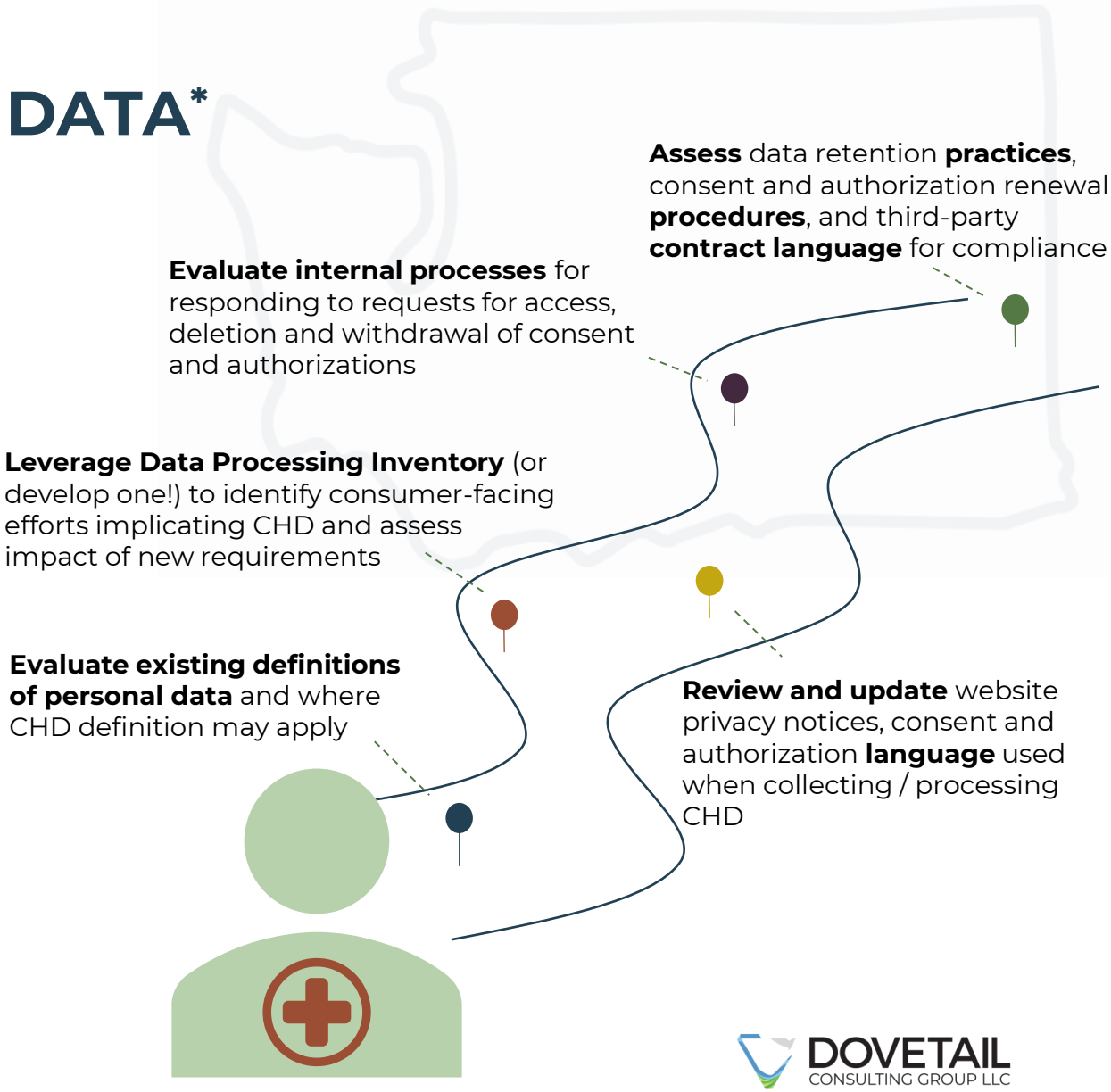
DOVETAIL
CONSULTING GROUP LLC

preview

WASHINGTON MY HEALTH MY DATA*

March 2024 (June 2024 for small businesses)

Consumer Health Data (CHD)	Broad definition that can include information derived or extrapolated from non-health data when used to associate consumers with consumer health data
No Applicability Thresholds	Applies to all legal entities ("Regulated Entities") conducting business in WA or, producing or offering products or services to WA consumers
Right to be Forgotten / Deletion	Virtually iron-clad. Potential for conflict with other legal obligations to retain information; 30-days to comply
Consent for use of CHD	Affirmative consent required for collection / processing of CHD, unless necessary to provide product or service requested by consumer
Consumer Health Data Privacy Policy (Notice)	Regulated Entities must provide a link on its homepage specific to CHD
Sale of CHD	Prohibited without explicit authorization (1 yr. expiry) that is separate or distinct from consent to use / share CHD, including name / contact information of purchaser



DOVETAIL CONSULTING GROUP LLC

* Examples only / not intended to provide comprehensive overview of legal requirements

Q&A

DOVETAIL
CONSULTING GROUP LLC

DOVETAIL
CONSULTING GROUP LLC

THANK YOU

privacy@dovetailcg.com