How to Gain Clients' Trust in Managing Their Data

Presented by Kadian Douglas & Phillip Del Bello

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

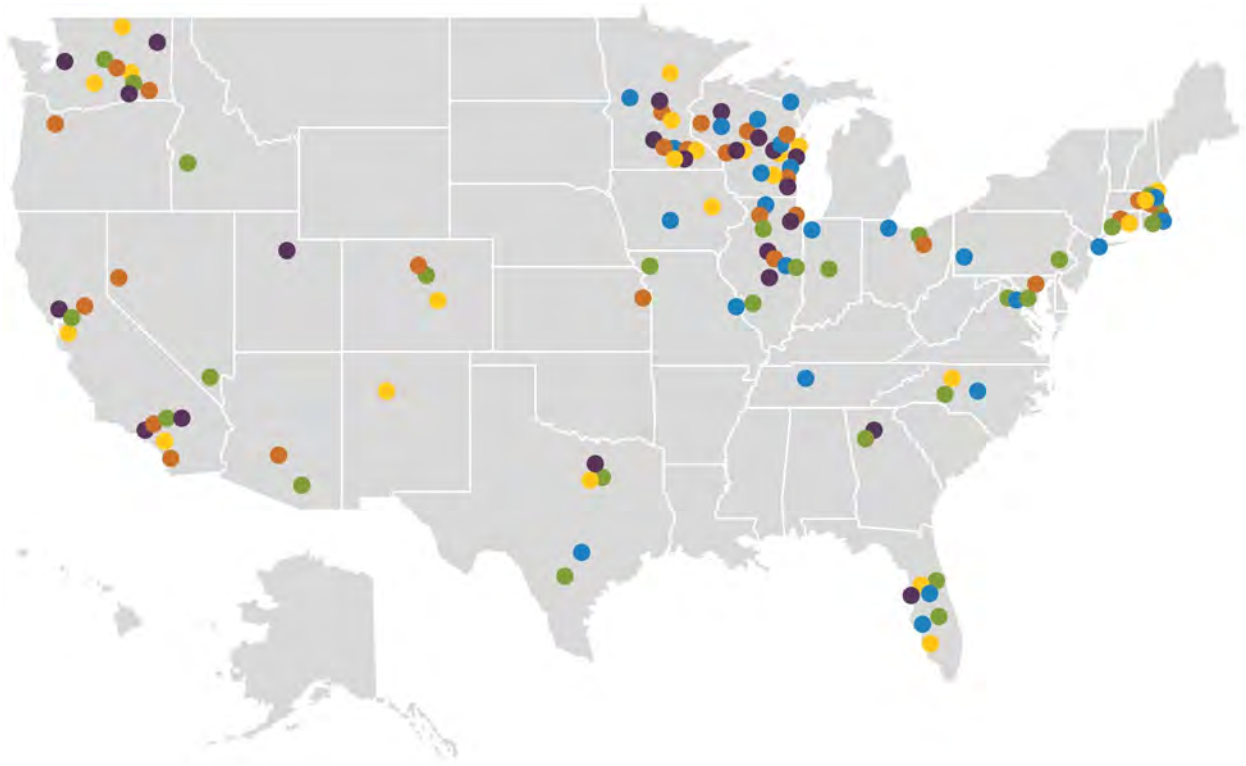
Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

About CLA


More than 120 locations
900+ principals
14 industries
7,400+ people
60 years and counting
Seamless, integrated capabilities

National and International Reach



A member of Nexia International

CLA has 7,400 professionals, operating from more than 120 locations across the country.

Agenda

1) **Risk of sharing data**
2) **Options for independent assessments**
3) **Various data Privacy compliance requirements and best practices**

Risk of Sharing Data

Compliance

- Countless regulatory requirements and ever-growing privacy requirements
- Covered entity must notify the HHS for breach of unsecured protected health information affecting 500 or more individuals, and may be liable for breaches of their business associates
- Ability to continue doing business

Financial

- $8.64 Million – IBM Reported Average Cost of Data Breach 2020 in United States (https://www.ibm.com/security/data-breach)
- Ability to continue doing business

Reputational

- 59% experienced a data breach caused by one of their third parties (https://www.ponemon.org/userfiles/filemanager/nvqfztft3qtufvi5gl60/)
- Ability to continue doing business

How to Gain Trust

Solid Security Practices and Culture

- Cybersecurity Risk Management Program
- Data Classification and Inventory
- Incident Response Plan
- Security Awareness Training
- Test, Test, Test

Independent Assessments

- SOC 2
- HITRUST
- ISO27001
- PCI DSS
- NIST Cybersecurity

Strong Reputation

- Staying out of the "Headlines"

Security Questionnaires

- Often required for due diligence

Independent Assessments

SOC 2

What is it?

- Reporting framework under AICPA SSAE 18
- System and Organization Controls (SOC)
- Not a certification, but attestation report

What is the scope?

- Description Criteria – AICPA Description of a Service Organization's System
- Trust Service Criteria – Required control framework
  - Security (Common Criteria), Availability, Confidentiality, Processing Integrity, Privacy
- Type 1: Point in time report (design of controls)
- Type 2: Testing over a period (effectiveness of controls)
- SOC 2+: Can add any other framework that is generally available, commonly see HIPAA Security Rule

SOC 2

Who is it for?

- Service Organizations – An organization that accesses, processes, or maintains data on behalf of another organization
- Designed for all service organization in all industries
- Designed to meet broad range of customers

What is the result?

- Typically, performed every year
- Auditor opinion in report can be unqualified, qualified, or adverse
- Opinion is provided on 3 areas:
  - Presentation of the "System Description" (Type 1 &2)
  - Design of the control activities (Type 1 &2)
  - Effectiveness of the control activities (Type 2)

HITRUST

What is it?

- HITRUST is an organization that includes a for-profit division (HITRUST Services Corp) and a not-for-profit division (HITRUST Alliance)
- Founded in 2007 to address the need for a security certification in the healthcare industry
- HITRUST CSF: Information security and privacy framework built on other standards / sources
- Certification issued by HITRUST

What is the scope?

- Scoped based on organizational, technical, and regulatory factors
- Incorporates more than 40 security and privacy related regulations, standards, and frameworks providing comprehensive and prescriptive coverage
- Covers 19 domains including every aspect of your security posture
- Assesses the Requirement Statements at 5 maturity levels
  - Policy, Process, Implemented, Measured, Managed

HITRUST

Who is it for?

- Originally for organizations that deal with ePHI
- Most common for organizations contracting with insurance providers or large health plans
- *In 2019, more than 90 payers and other healthcare industry companies require their third-party service providers (business associates) to become HITRUST certified.* – Healthcare Weekly
- Now can be applicable to all industries

What is the result?

- Goal is to obtain HITRUST Certification
- Certification good for 2 years, with interim assessment
- Can also demonstrate compliance with:
  - HIPAA, NIST 800-171, CMMC, FISMA, GDPR, CCPA

Comparing HITRUST and SOC 2

	SOC 2 Type 2	HITRUST Validated Assessment
Scope	- Required Security Trust Service Criteria – Common Criteria - TSC follows COSO Framework - Less prescriptive requirements (33 in Common Criteria) - Considers risks of your organization to define controls, on average includes 70-100 - Report is Unqualified or Qualified, with exceptions - Option for SOC 2 +	- Based on MyCSF Factors and optional regulatory frameworks - Typically, minimum of 250 requirements, up to several hundred - Detailed requirement statements and illustrative procedures - Certification is based on average score - Built on ISO 27001 and NIST, but can include many other regulatory frameworks

Comparing HITRUST and SOC 2

	SOC 2 Type 2	HITRUST Validated Assessment
Timing	SOC 2 Readiness Assessment - 2 to 3 months SOC 2 Type 2 - 6 to 12 months reporting period - 1 to 2 months for reports issued after period end - Full audit every year	HITRUST Readiness Assessment - 3 to 4 months HITRUST Validated Assessment - Control, policies, and procedures should be established for at least 90 days - Full assessment every 2 years, Interim assessment second year - 2 to 4 months for HITRUST QA and certification issued

Comparing HITRUST and SOC 2

	SOC 2		HITRUST Validated Assessment	
	Phase	**Potential Costs**	**Phase**	**Potential Costs**
External Assessment Cost	SOC 2 Readiness Assessment	To be discussed	HITRUST Readiness Assessment	To be discussed
	SOC 2 Type 1	To be discussed	HITRUST Validated Assessment (Certification)	To be discussed
	SOC 2 Type 2	To be discussed	HITRUST Interim Assessment	To be discussed
			HITRUST MyCSF Subscription	TBD by HITRUST
			HITRUST Reporting Fee	TBD by HITRUST

SOC 2 + HITRUST Option

- An opinion on the suitability of the design and operating effectiveness of the controls based on
  - The applicable trust services criteria and
  - The HITRUST CSF criteria as scoped to the service organization
- “Under this structure of reporting, the SOC 2 + HITRUST report becomes the default method of reporting to meet the widest range of requests.” - HITRUST

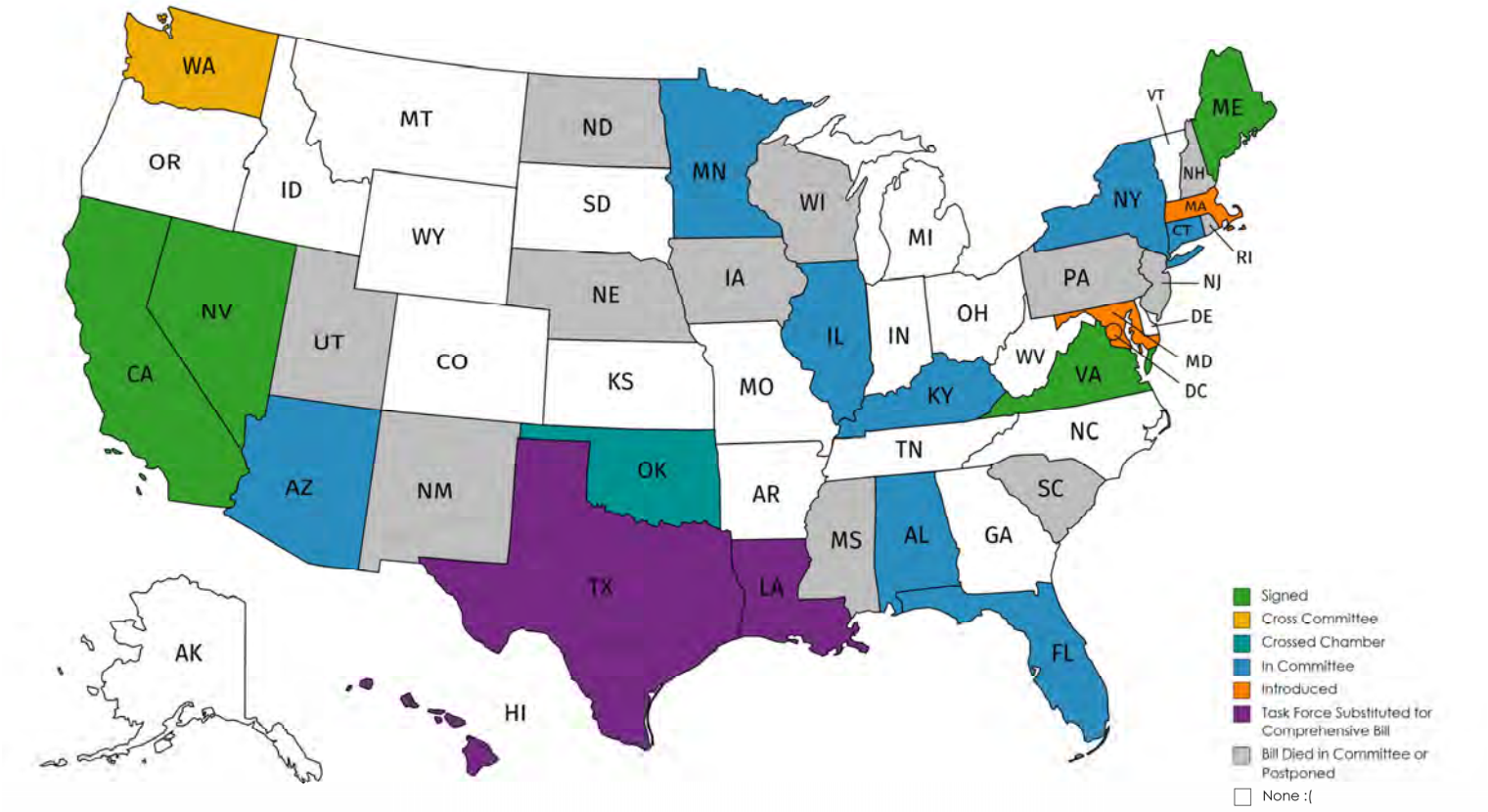
Which One Should I Choose?

- **Industry and Strategic Goals**
  - Specific industries have specific frameworks that may be preferred/required
  - If you serve a broad range of industries, SOC 2 may cover all
- **Organization Size and Budget**
  - Each independent assessment option will have different costs associated
- **Contractual Requirements**
  - Assess current contractual requirements to provide independent assessment reports
  - Plan for future contracts to ensure your current option will work
  - *Customers may ask for one type of report, but are willing to accept others*

HITECH Act Amendment

- Signed January 5, 2021
- The bill requires the HHS to consider an entity's use of **recognized security best practices** when investigating reported data breaches and considering HIPAA enforcement penalties or other regulatory actions.
- "decreasing the length and extent of an audit under section 13411, or remedies otherwise agreed to by the Secretary, the Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices"
- **https://www.congress.gov/bill/116th-congress/house-bill/7898/**

U.S. Consumer Data Privacy Laws



As of March 8, 2021

Current Data Privacy Regulations

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Vertically-Focused U.S. Privacy Laws

- **U.S. Privacy Act of 1974**
- **Family Educational Rights and Privacy Act (FERPA)**
- **Gramm-Leach Bliley Act (GLBA)**
- **Children's Online Privacy Protection Act (COPPA)**
- **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule**

Comprehensive Consumer Privacy Regulations

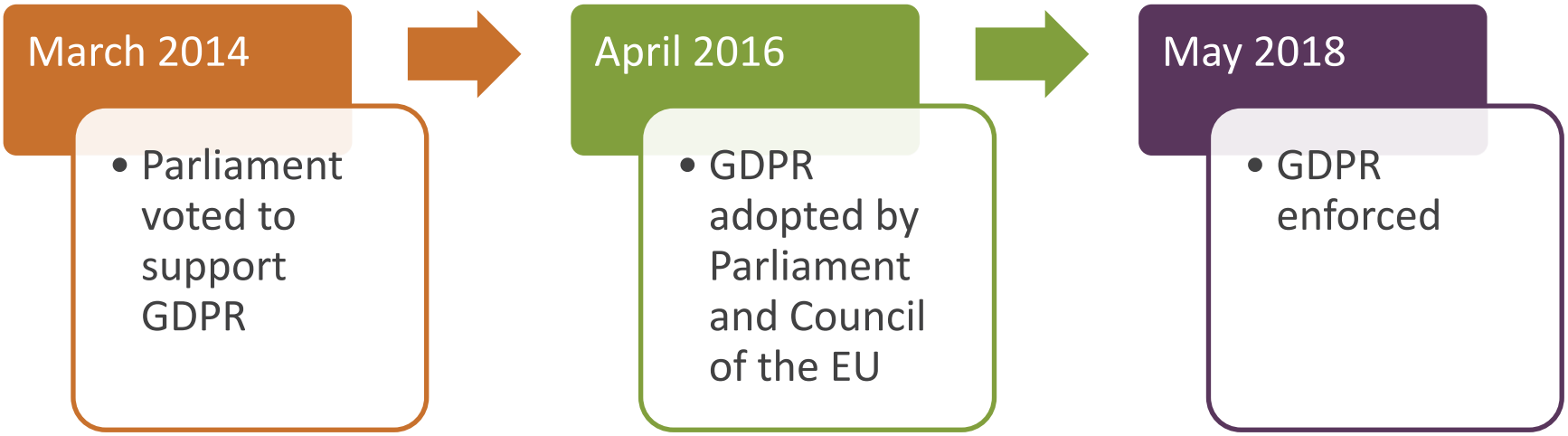
- **EU's General Data Protection Regulation (GDPR)**
- **California Consumer Privacy Act (CCPA)**
- **Emerging U.S. and International regulations**

General Data Protection Regulation (GDPR)

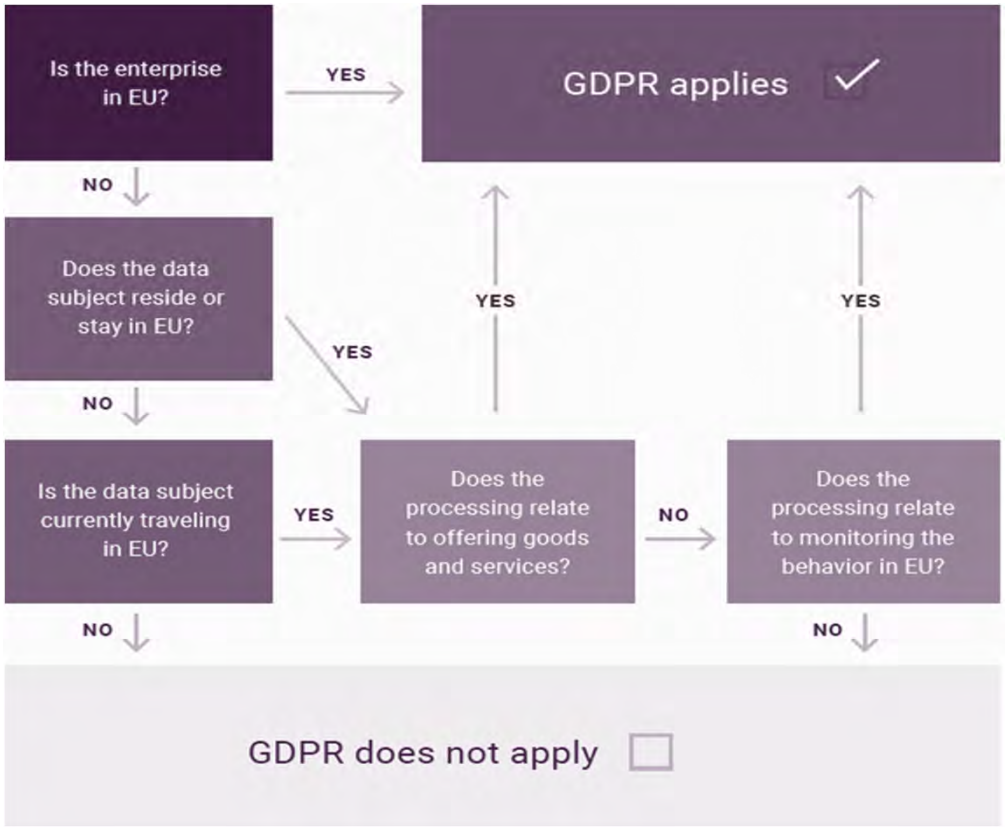
WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

What is it?

Europe's framework for data privacy



Does GDPR Apply to my Organization?



Key Provisions

Data Subject Rights

- The right to be informed
- The right of access
- The right to rectification
- The right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Data Breaches

Breach

- Loss, alteration, destruction, or unauthorized disclosure of or access to personal data

Notification

- Must be given within 72 hours of a breach
- Includes as many forms as deemed necessary to distribute the information in a timely manner

Penalties

- **Maximum penalty for noncompliance is up to €20 million ($23,230,820) or 4% of annual revenue (whichever is greater)**
  - Consent
  - Privacy by Design
- **Other violations are assessed on a tiered basis depending on the infraction, up to €10 million ($10,854,150) or 2% of annual revenue (whichever is greater)**

California Consumer Privacy Act (CCPA)

California Privacy Rights Act (CPRA)

CCPA Consumer Rights

- Right to Know
- Right to Deletion
- Right to Opt Out
- Right to Antidiscrimination
- Required Notices

Timelines

California Consumer Privacy Act (CCPA)

June 28, 2018

CCPA signed into law

January 1, 2020

CCPA took effect

July 1, 2020

Attorney General began enforcement

California Privacy Rights Act (CPRA)

November 3, 2020

CPRA approved by California voters

January 1, 2023

CPRA takes effect

July 1, 2023

CPRA begins enforcement

Scope

CCPA	CPRA
(1) $25+ million in annual revenue; (2) buys or sells, OR receives or shares for business's **commercial purpose**, PI of **50,000+ consumers, households or devices**; or (3) derives at least 50% of annual revenue from selling consumer PI.	(1) $25+ million in annual revenue; (2) buys, sells or shares PI of **100,000+ consumers or households**; or (3) derives at least 50% of annual revenue from selling **or sharing** consumer PI.

CPRA: Expanded Consent Requirements

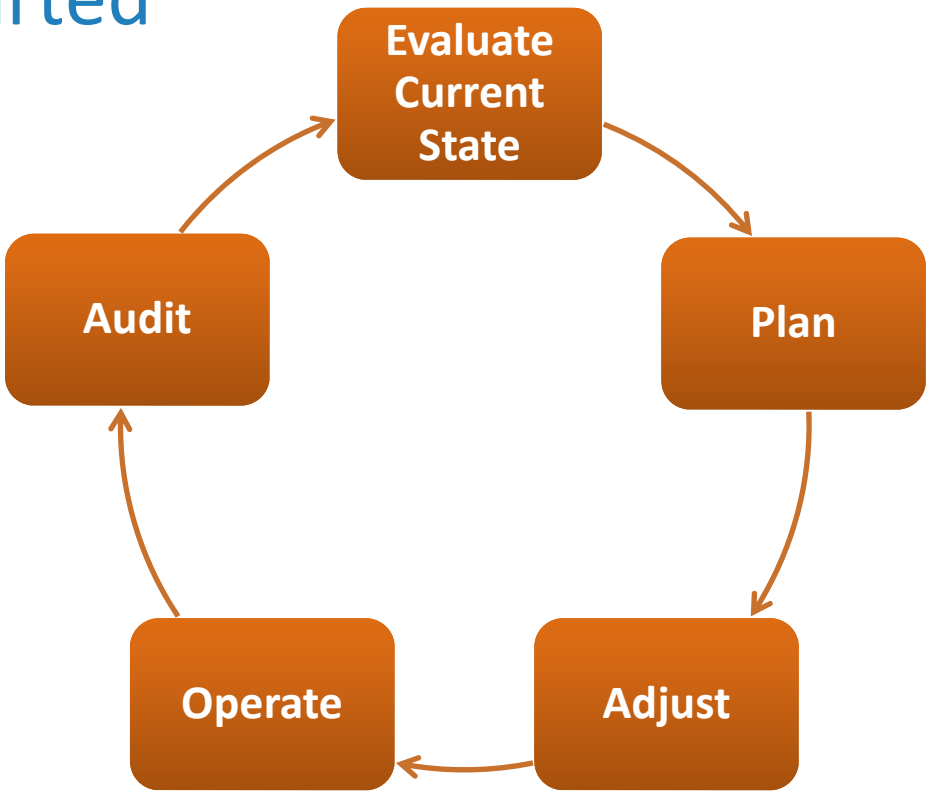
- **Selling or sharing personal information after a user has already opted out**
- **Selling or sharing the personal information of minors**
- **Secondary use, selling or sharing of sensitive personal information after a user has opted out**
- **Research exemptions**
- **Opt-in to financial incentive**

Improving Your Privacy Compliance Program

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Getting Started



Evaluate Current State

- **Perform a data audit and gap assessment**
- **Identify weaknesses in security**
  - Including data storage and transfers
- **Determine if third parties are compliant with privacy requirements**
- **Goals:**
  - Understand current gaps
  - Develop a remediation plan

Questions You Should Ask

- **Does the regulation apply to us?**
- **Who is protected?**
- **What rights do they have?**
- **What is personal information?**
- **What personal information do we have?**
- **How is the regulation enforced?**
- **Can we be sued?**

Design and Plan

- **Using the gap assessment and remediation plan; develop controls, policies and procedures to narrow the gap**
- **Goals:**
  - Address and correct any data deficiencies
  - Update policies, procedures, and contracts
  - Implementation plan

Adjust

- **Implement the remediation plan**
- **Provide training to employees on adjustments**
- **Goals:**
  - New controls, policies, and procedures implemented

Operate

- **Monitor fully implemented processes for a defined period of time (Recommend 3-6 months) and assess the effectiveness of the new operational framework**
- **Goals:**
  - Evaluate the effectiveness of the controls, processes, and procedures and make necessary tweaks

Audit and Repeat as Necessary

- **Monitor activity, evaluate overall compliance, document appropriate evidence, and report compliance as necessary based off data population and usage**
- **Goals:**
  - Meet the requirements of applicable Laws/Regulations that apply to the processing of personally identifiable information and associated data

Building a Privacy Compliance Program

Ongoing Security and Data Management Practices

Thank you!

Phillip Del Bello
Phillip.DelBello@CLAconnect.com

Kadian Douglas
Kadian.Douglas@CLAconnect.com

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING