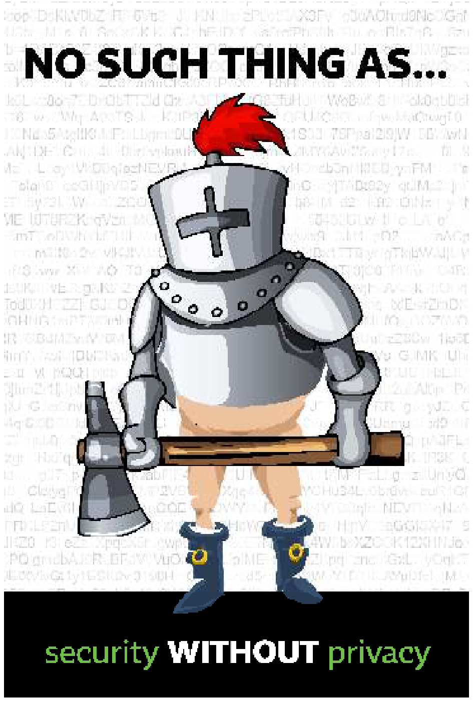
Modern Approach to Privacy Impact Assessments

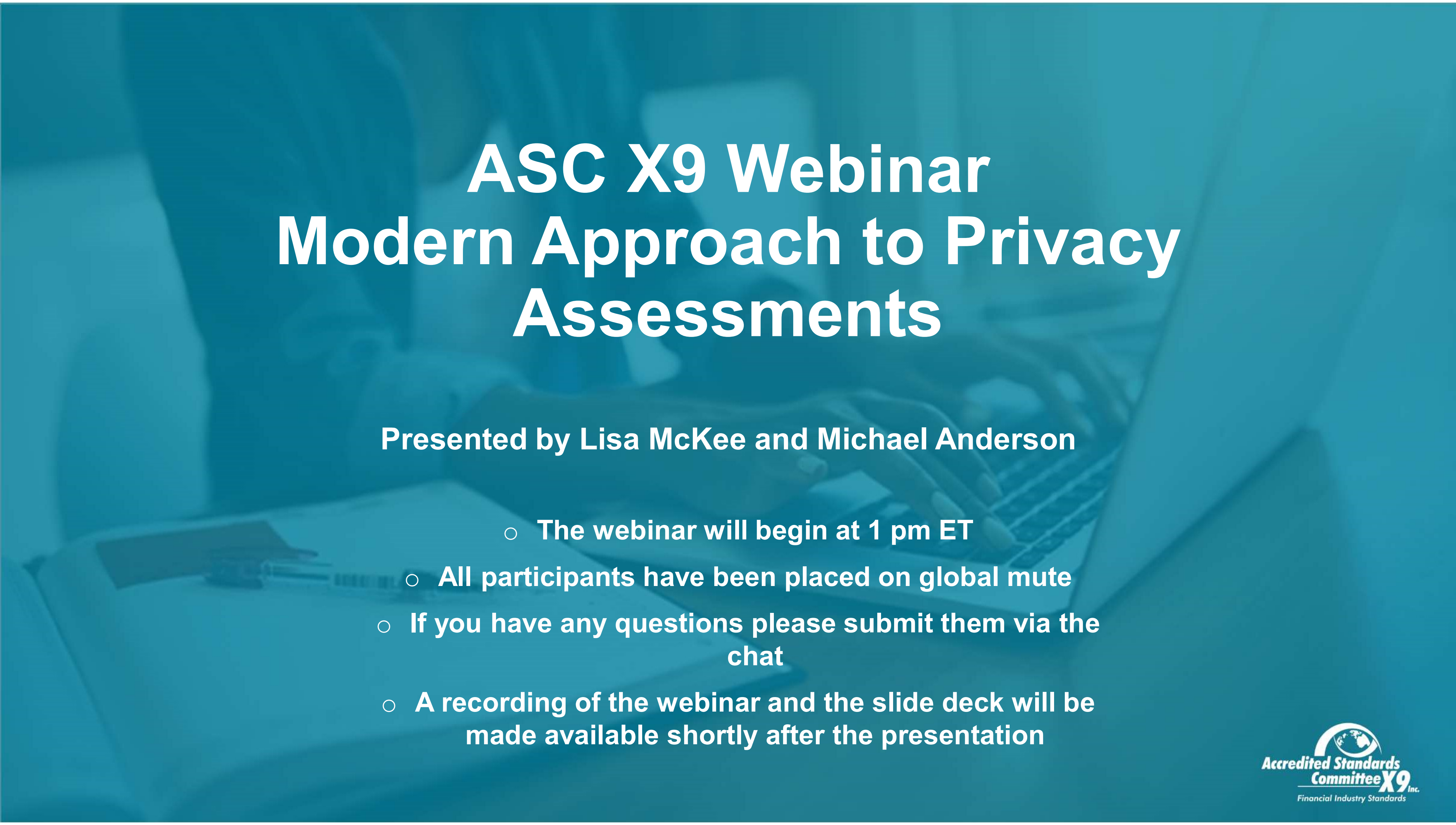
Lisa McKee & Michael Anderson

April 29, 2021

Welcome to

ASC X9





ASC X9 Webinar
Modern Approach to Privacy Assessments

Presented by Lisa McKee and Michael Anderson

- The webinar will begin at 1 pm ET
- All participants have been placed on global mute
- If you have any questions please submit them via the chat
- A recording of the webinar and the slide deck will be made available shortly after the presentation

Accredited Standards Committee X9 Inc.
Financial Industry Standards

Session Speakers

Lisa McKee,
CISA, CDPSE, PCIP

Senior Manager
Protiviti

PROUD MEMBER OF
Accredited Standards Committee X9 Inc.
Financial Industry Standards

Michael Anderson
CGEIT | CISSP | CISA | CRISC | CDPSE |
CAP | HCISPP | PCI-QSA | PCIP | CCSFP |
CHQP | Security+ | Network+

Senior Consultant
CompliancePoint

Today’s topics

What are PIA/DPIAs

Their similarities and differences

How to conduct a PIA/DPIA

Tools, Templates, Resources

What is Privacy?

What is the difference between security and privacy?

- Security focuses on unauthorized access to data.
- Privacy can be authorized access that violates expectations in the use and processing of data.

Categories of Personal Information

Is It Personal Data?

Personal Identifiers/ Biometric Data

Individual Profile

Health Insurance/ Medical Records

Online Activity

Financial Records/ Purchasing Information

Protected Characteristics

Education, Professional, Employment Data

Geolocation Data

Privacy Across the Organization

Privacy Impacts Everyone

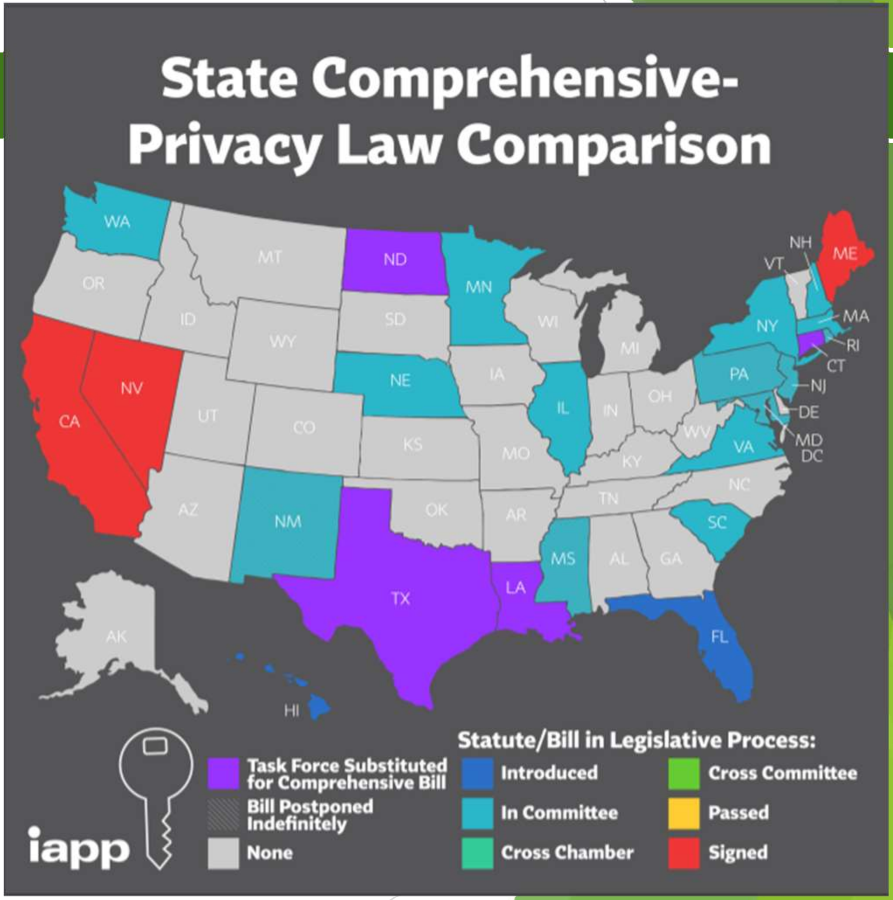
- Information Technology
  - Accessibility limitations
  - Database management
  - Asset inventory
  - Virtual machines
  - System availability
  - Processing Activities
- Human Resources
  - Compensations and benefits
  - Talent acquisition/hiring
  - Employee records
  - Training and development
  - Performance Management
  - Succession Planning
  - Social media
  - Remote employees/BYOD
- Information Security
  - IT systems
  - Building security
  - Remote users
  - Vendors
  - Third Parties
- Legal and Compliance
  - Privacy practices
  - Ethics statements*
  - Whistleblowing*
  - Investigations*
  - Audit, risk, compliance (may be separate)
- Marketing/Business Development
  - Digital advertisement
  - Cookies/consent
- Finance
  - Payroll
  - Securities and investments
  - Travel expense reimbursement
  - Accounts Receivable
  - Accounts Payable
- Other Stakeholders
  - Employees
  - Processors/Third Party Vendors
  - Consumers
  - Policymakers/Regulators

* May be done by HR or Legal

Privacy Laws and Standards

Pre-Covid

- X9.99 PIA Standard 2009/2020
- ISO 22307 PIA Standard 2009/2020
- GDPR Regulation May 2018
- ISO Privacy Standard in 2019
- California (CCPA) July 2020
- NIST Privacy Standard January 2020



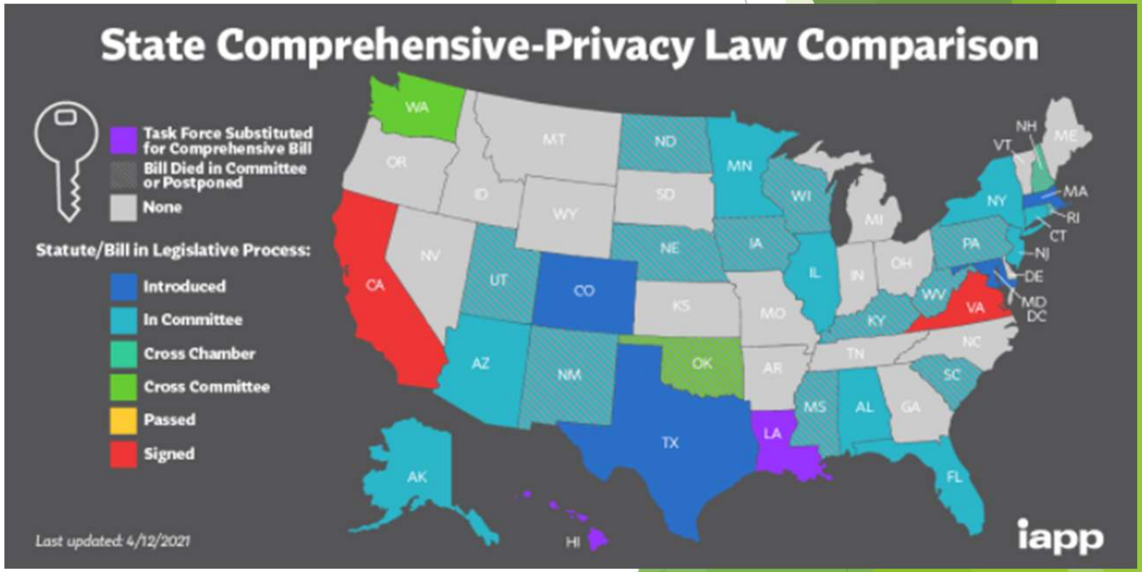
State Comprehensive-Privacy Law Comparison

Privacy Laws and Standards

Post Covid

- *11/03 – California **Passed** (CPRA Jan 1 2023)
- *1/05 – Washington Privacy
- 1/06 – New York Biometric
- *1/06 – New York Privacy
- *1/07 – Minnesota Privacy
- 1/15 – Connecticut Privacy
- 2/01 – Oklahoma Privacy
- 2/16 – Utah Privacy
- *2/17 – Illinois Privacy
- 2/26 – Rhode Island Privacy
- *3/02 – Virginia Privacy **Passed** (VCDPA Jan 1 2023)
- *3/11 – Utah Cybersecurity
- 3/15 – National Privacy Law
- *3/19 – Colorado Privacy
- 3/22 – Texas Privacy
- 4/01 – Alaska Privacy

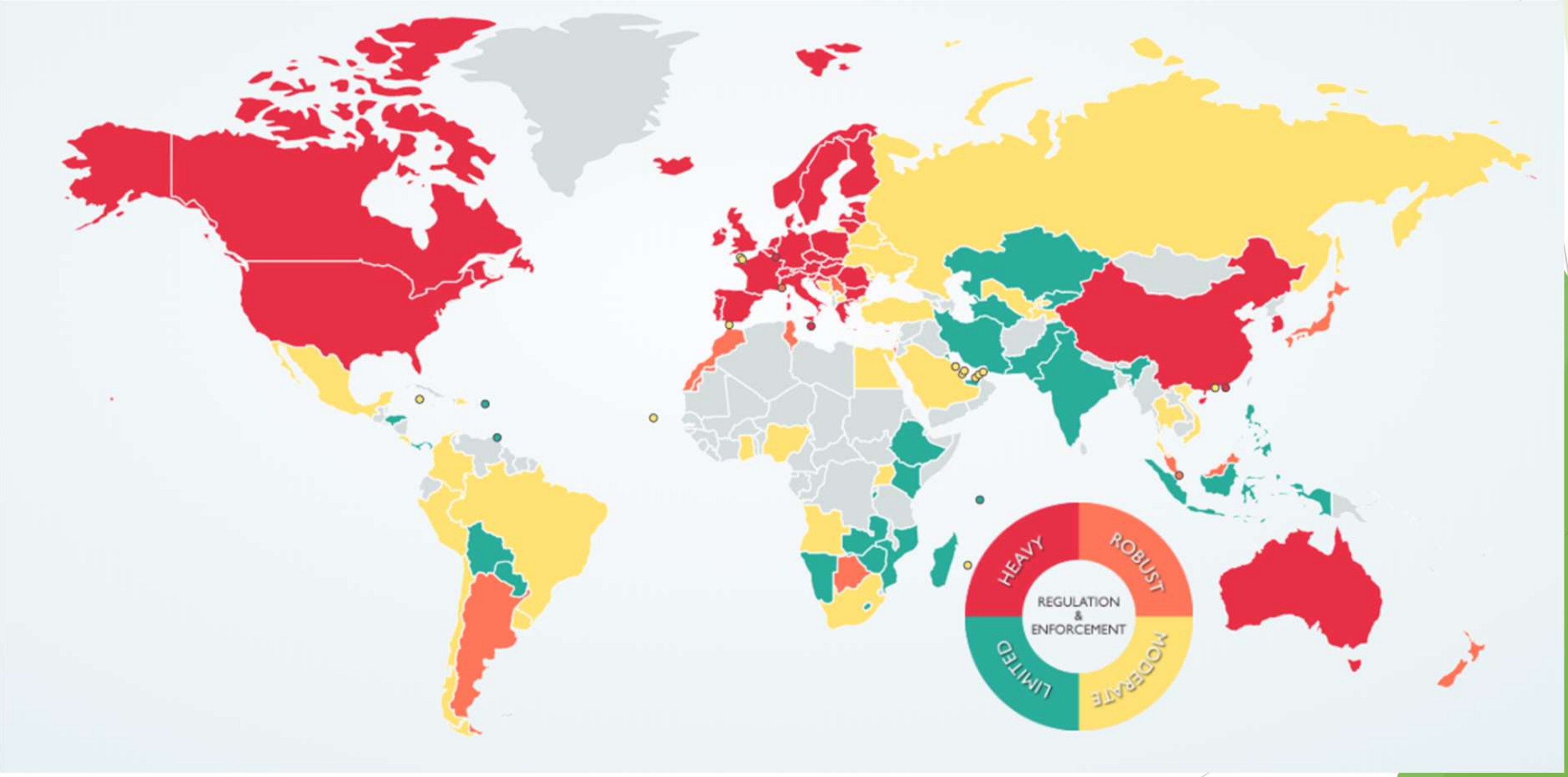
- *Risk Assessment Requirements



https://iapp.org/resources/article/state-comparison-table/#

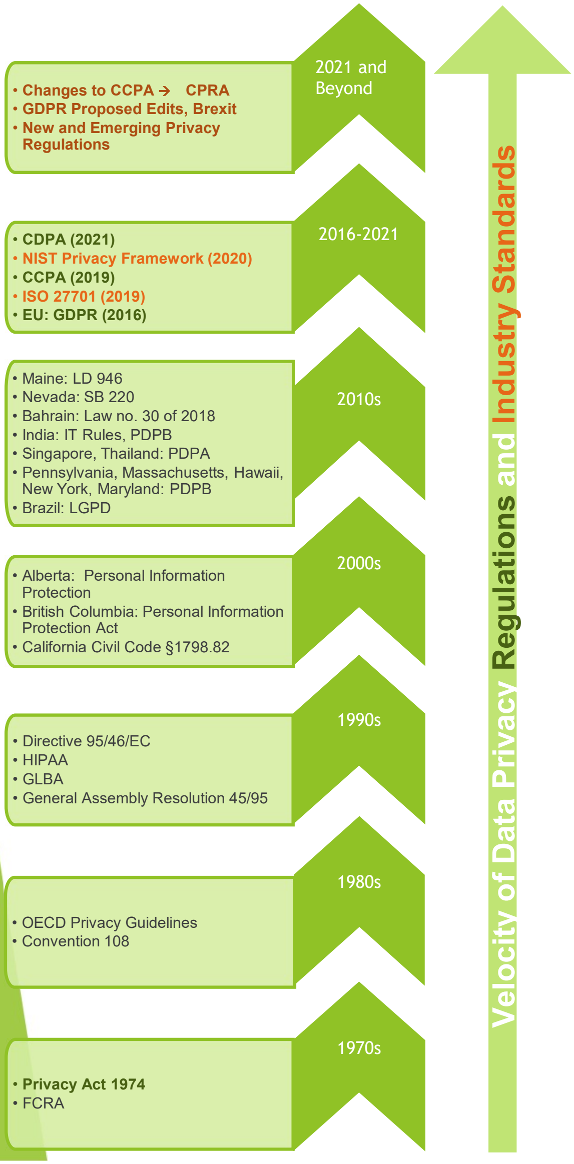
Global Privacy laws

International Privacy Laws



https://www.dlapiperdataprotection.com/

Evolution of Data Breaches



2021 and Beyond
- Changes to CCPA → CPRA
- GDPR Proposed Edits, Brexit
- New and Emerging Privacy Regulations

2016-2021
- CDPA (2021)
- NIST Privacy Framework (2020)
- CCPA (2019)
- ISO 27701 (2019)
- EU: GDPR (2016)

2010s
- Maine: LD 946
- Nevada: SB 220
- Bahrain: Law no. 30 of 2018
- India: IT Rules, PDPB
- Singapore, Thailand: PDPA
- Pennsylvania, Massachusetts, Hawaii, New York, Maryland: PDPB
- Brazil: LGPD

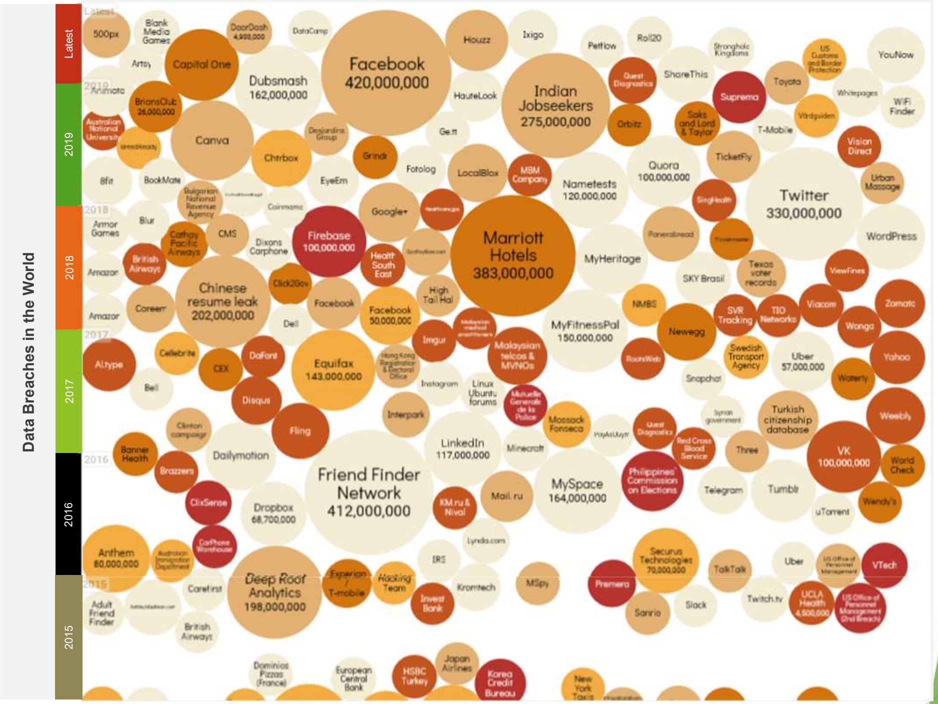
2000s
- Alberta: Personal Information Protection
- British Columbia: Personal Information Protection Act
- California Civil Code §1798.82

1990s
- Directive 95/46/EC
- HIPAA
- GLBA
- General Assembly Resolution 45/95

1980s
- OECD Privacy Guidelines
- Convention 108

1970s
- Privacy Act 1974
- FCRA

Velocity of Data Privacy Regulations and Industry Standards



↑ **Volume of Data Breaches/Incidents**

→ **Velocity of Data Privacy Regulations**

Privacy regulations across the globe have developed more in the past 12 months than they have in the preceding century, leaving many organizations confused and unable to adapt their privacy programs at a suitable pace. The volume and value of sensitive data records stolen have also increased this period.

Source(s): Gartner: The State of Privacy and Personal Data Protection 2019-2020, The Keys to Data Protection

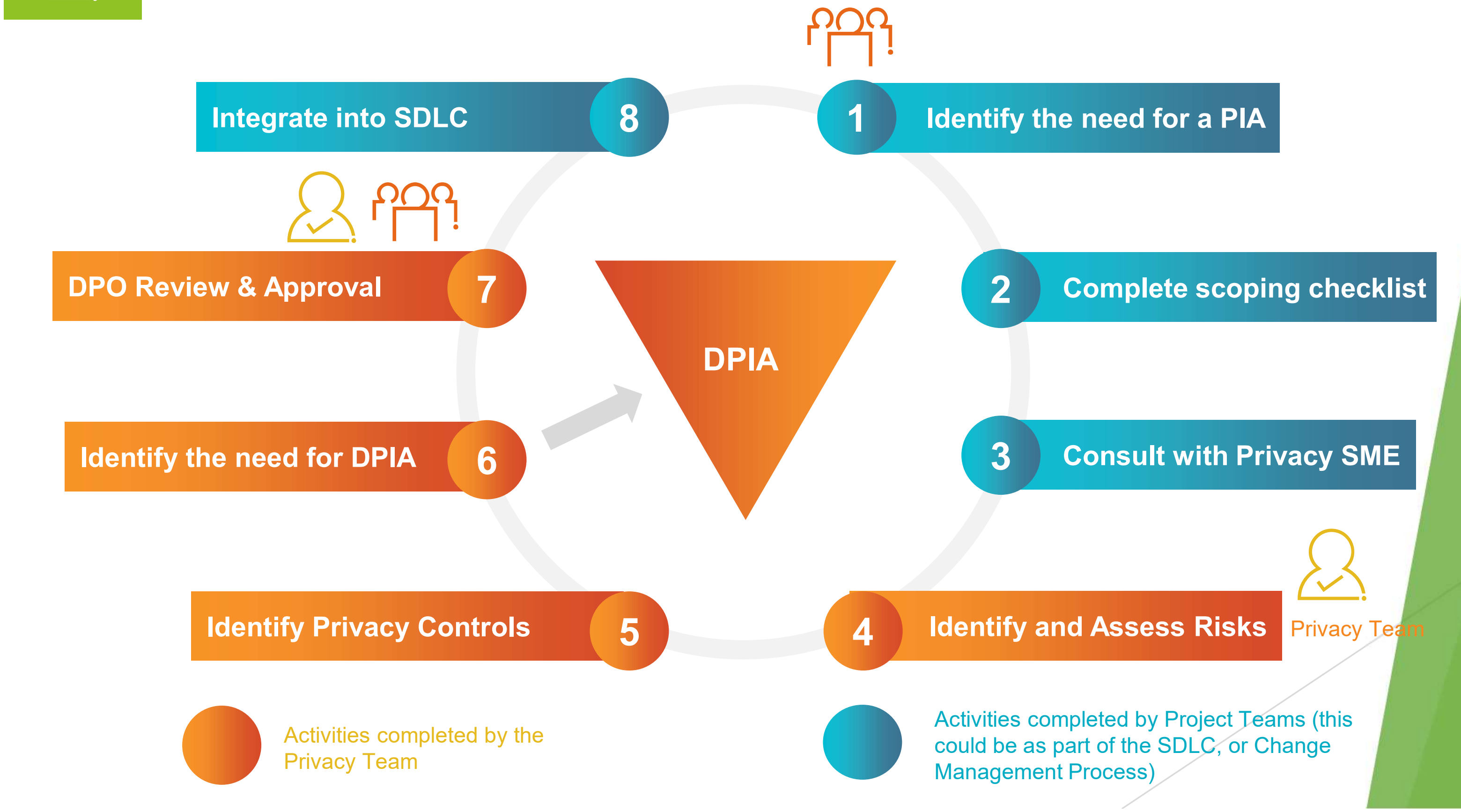
PIA vs. DPIA

Similarities and Differences

- PIA
  - Analyzing risks associated with how an entity collects, uses, shares and maintains personally identifiable information.
  - Process used to inform Privacy by Design when an organization starts or acquires a new business, implements a new process or launches a new product.
- DPIA
  - Identifying and minimizing risks associated with **high-risk processing** of personal data.
  - An on-going process, regularly applied to personal data processing, identifying and mitigating risks.

PIA Process

Performing a Privacy Impact Analysis (PIA) and when applicable, a Data Protection Impact Assessment (DPIA) together with the documentation on decisions taken with regard to the results, is a good beginning to establish the privacy requirements that must be implemented in applications and systems as part of privacy by design, as well as to fully document how personal data is processed, and follow the principle of accountability.



1 Identify the need for a PIA

2 Complete scoping checklist

3 Consult with Privacy SME

4 Identify and Assess Risks

Privacy Team

5 Identify Privacy Controls

6 Identify the need for DPIA

7 DPO Review & Approval

8 Integrate into SDLC

DPIA

🟧 Activities completed by the Privacy Team

🟦 Activities completed by Project Teams (this could be as part of the SDLC, or Change Management Process)

Key Elements of a DPIA

7 Steps for Conducting a DPIA

- Step 1: identify the need for a DPIA
- Step 2: describe the processing
- Step 3: consider consultation
- Step 4: assess necessity and proportionality
- Step 5: identify and assess risks
- Step 6: identify measures to mitigate the risks
- Step 7: sign off and record outcomes

Key Elements of a DPIA

Step 1: Identify the Need for a DPIA

- Explain broadly what project aims to achieve and what type of processing it involves.
- You may find it helpful to refer or link to other documents, such as a project proposal.
- Summarize why you identified the need for a DPIA.

Key Elements of a DPIA

Step 2: Describe the Processing

- Describe the nature of the processing
- Describe the scope of the processing
- Describe the context of the processing
- Describe the purposes of the processing

High Risk Processing Criteria

As defined by Article 35 of the GDPR, “high-risk” processing activities require completion of the Data Protection Impact Analysis (DPIA). The table below outlines threshold criteria to be considered when to identify high-risk processing activities and determine if completion of a DPIA is necessary.

No.	Threshold Criteria	Criterion Considerations
1	Evaluation or scoring	Profiling and predicting, especially from “aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements” (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioral or marketing profiles based on usage or navigation on its website.
2	Automated-decision making with legal or similar significant effect	Processing that aims at taking decisions on data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person” (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.
3	Systematic monitoring	Processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area” (Article 35(3)(c))15. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).
4	Sensitive data or data of a highly personal nature	This includes special categories of personal data as defined in Article 9 (for example information about individuals’ political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients’ medical records or a private investigator keeping offenders’ details.

High Risk Processing Criteria

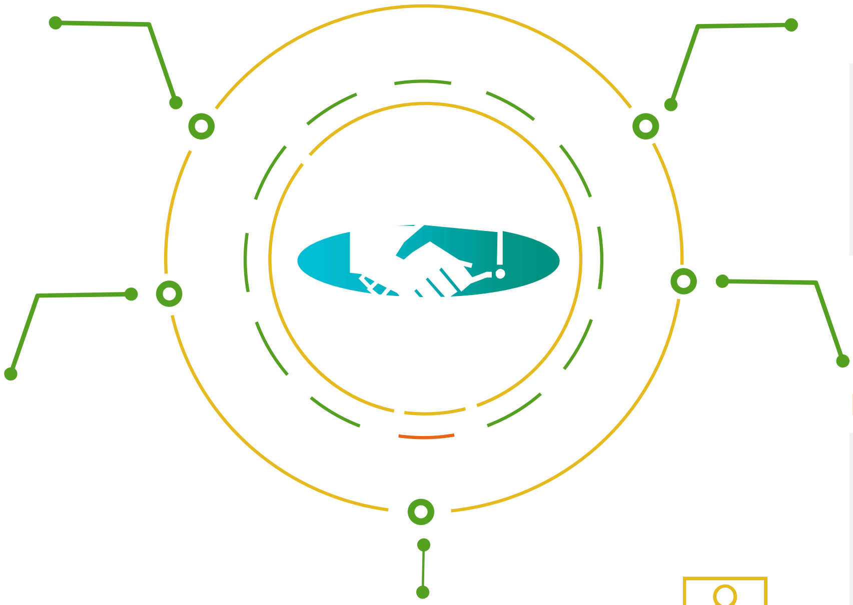
No.	Threshold Criteria	Criterion Considerations
5	Data processed on a large scale	Processing on a large sale is not defined but the GDPR; however, the following guidance has been provided by the Data Protection Authorities (DPAs) when determining whether the processing is carried out on a large scale • the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; • the volume of data and/or the range of different data items being processed; • the duration, or permanence, of the data processing activity; • the geographical extent of the processing activity.
6	Matching or combining datasets	This criteria highlights processing that originates from "two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject."
7	Processing data concerning vulnerable data subjects (i.e. children)	Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees , more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
8	Innovative use or applying new technological or organizational solution	Examples of new technologies that meet this criteria are: • Combining use of fingerprint and face recognition for improved physical access control. • Contact tracing technologies for tracking individuals that have been exposed to a disease or a virus.
9	Processing prevents a right or the use of services/products	When the processing in itself “prevents data subjects from exercising a right or using a service or a contract” (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

Key Elements of a DPIA

Step 3: Consider Consultation

- Consider how to consult with relevant stakeholders:
  - describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so.
  - Who else do you need to involve within your organization?
  - Do you need to ask your processors to assist?
  - Do you plan to consult information security experts, or any other experts?

Step 3: Privacy Stakeholders



Privacy Office

Responsible for overseeing the Privacy Program, including embedding “Data Protection by Design and by Default” into the design and operation of an organization’s IT operational infrastructure and business practices.

Project Management Office (PMO)

Responsible for embedding “Data Protection by Design and by Default” into projects at the outset by including deliverables such as contributing PTA/PIA/DPIA during the appropriate phases of the SDLC process, promoting accountability across projects and ensuring appropriate oversight of vendors/service providers.

Information Technology (IT)

Responsible for considering privacy issues at all phases of the design and development of products and systems and ensuring the organization maintains comprehensive data management procedures, including providing relevant privacy and security training to employees and regularly assessing the privacy and security impact of projects. These responsibilities may be shared with Information Security (IS).

Information Security (IS)

Responsible for and implementing privacy and security measures, such as pseudonymization and encryption and contributing to PTA/PIA/DPIA during the appropriate phases of the SDLC process. These responsibilities may be shared with IT.

Business Stakeholders

Responsible for defining the business requirements with privacy in mind at the outset. Responsible for complying with the organization’s privacy policies, standards and procedures regarding the collection, use, retention and disposal of personal data.

Key Elements of a DPIA

Step 4: Assess Necessity and Proportionality

- Describe compliance and proportionality measures, in particular:
  - what is your lawful basis for processing?
  - Does the processing actually achieve your purpose?
  - Is there another way to achieve the same outcome?
  - How will you prevent function creep?
  - How will you ensure data quality and data minimization?
  - What information will you give individuals?
  - How will you help to support their rights?
  - What measures do you take to ensure processors comply?
  - How do you safeguard any international transfers?

Key Elements of a DPIA

Step 5 - Identify and Assess Risks

- Describe source of risk and nature of potential impact on individuals.
- Include associated compliance and corporate risks as necessary.

Privacy Risk

Is It Personal Data?

Overcollection of Data

Inappropriate Data Usage

Unfitting Data Retention Standards

AI/ML Bias in Decisioning

Ineffective Security/Privacy Controls

Lack of Policies & Procedures

No DPO/CPO

Missing Regulations

Key Elements of a DPIA

Step 6: identify measures to mitigate the risks

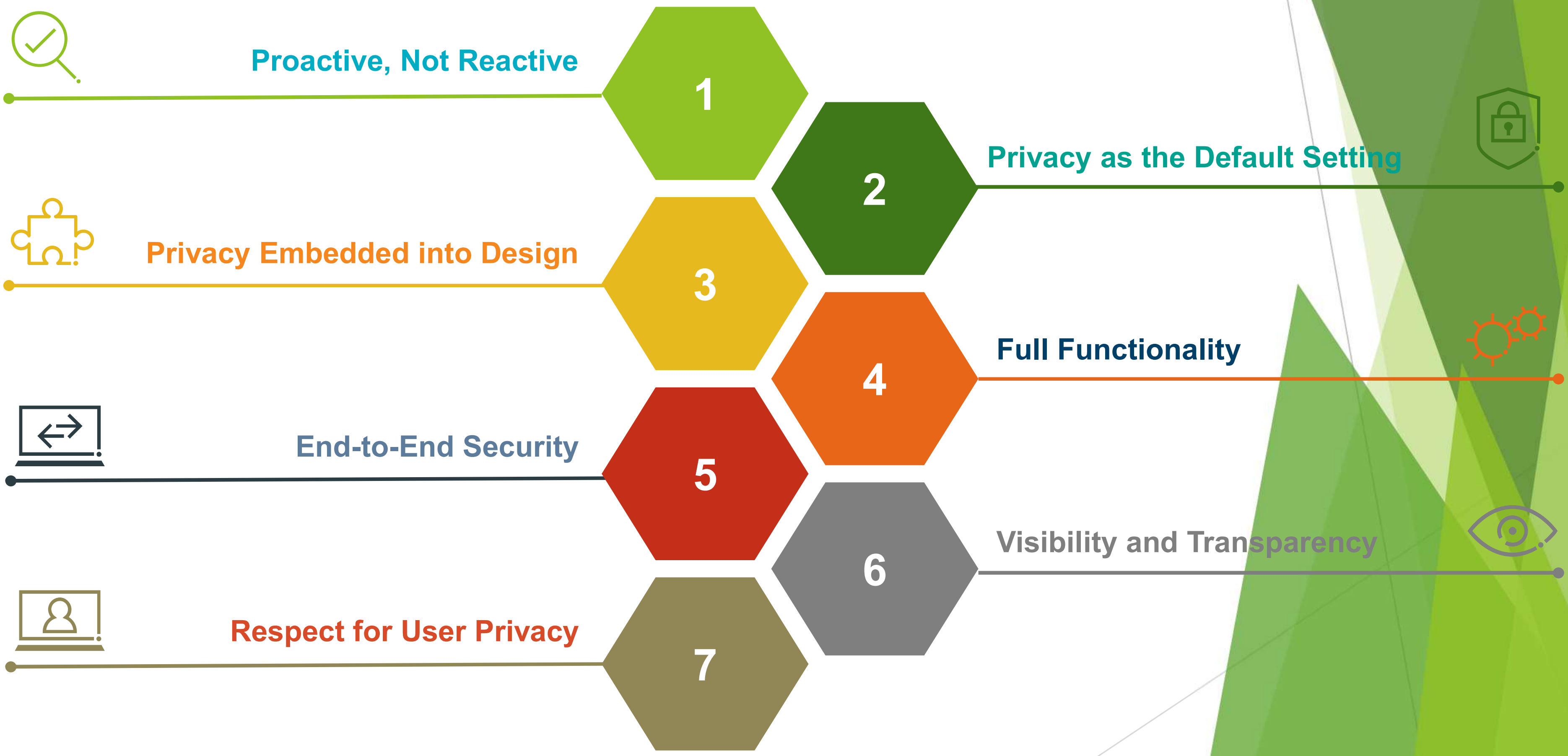
- Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Key Elements of a DPIA

Step 7 - Sign Off and Record Outcomes

- Measures
- Residual Risks
- DPO/CPO Advice:
  - Summary of DPO/CPO Advice
  - Actions Take (accepted/Overruled)
  - Comments
- Consultation Responses
- DPIA Owner

SDLC – Embedding PRIVACY BY DESIGN



1. Proactive, Not Reactive
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality
5. End-to-End Security
6. Visibility and Transparency
7. Respect for User Privacy

Privacy Tools & Resources

GRC SOLUTIONS

PRIVACY SOLUTIONS

SUBSCRIPTIONS

MEMBERSHIPS

INDUSTRY GROUPS

WEBINARS

TRAINING

References

Links to Privacy Materials

1. IAPP: The Schrems II Decision: EU-US Data Transfers in Question https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/
2. IAPP: https://iapp.org/
3. IAPP: US State comprehensive Privacy Law Comparison. https://iapp.org/resources/article/state-comparison-table/#
4. GDPR Personal Categories: https://dataedo.com/blog/what-is-personal-data-under-gdpr
5. CCPA Personal Categories: https://reciprocitylabs.com/resources/what-are-the-ccpa-categories-of-personal-information/
6. Global Privacy Laws: https://www.dlapiperdataprotection.com/
7. EU PIA Template: https://gdpr.eu/data-protection-impact-assessment-template
8. Article 29 : https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360
9. Washington Data Privacy Act: https://app.leg.wa.gov/billsummary?BillNumber=5062&Year=2021&Initiative=false
10. New York Biometric Privacy Act: https://legiscan.com/NY/text/A00027/2021
11. New York Privacy Act: https://legiscan.com/NY/bill/A00680/2021
12. Minnesota Privacy Law Proposed: https://www.hinshawlaw.com/newsroom-updates-data-cyber-bytes-minnesota-consumer-data-privacy-bill.html
13. Connecticut Consumer Privacy Act: https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB156&which_year=2021
14. Oklahoma Computer Data Privacy Act Proposed: https://www.insurancejournal.com/news/southcentral/2021/03/08/603859.htm
15. Utah Consumer Privacy Act: https://le.utah.gov/~2021/bills/static/SB0200.html
16. Illinois Right to Know Act: https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2404&GAID=16&DocTypeID=HB&LegId=131162&SessionID=110&GA=102
17. Rhode Island Proposed Data Privacy Act: http://webserver.rilin.state.ri.us/BillText18/HouseText18/H7111.htm
18. Virginia Data Protection Act: https://www.adexchanger.com/privacy/virginias-gov-signs-customer-data-protection-act-into-law/
19. Utah Data Security Law: https://le.utah.gov/~2021/bills/static/HB0080.html
20. National Privacy Law Proposed: https://www.cnbc.com/2021/03/10/democrat-delbene-proposes-national-privacy-standard.html
21. Colorado Protect Personal Data Privacy Bill: https://legiscan.com/CO/drafts/SB190/2021
22. Texas: https://www.house.texas.gov/
23. Alaska Privacy Bill: : https://lawstreetmedia.com/tech/alaska-governor-introduces-consumer-data-privacy-bill/#:~:text=On%20Wednesday%2C%20Alaska%20Gov.,of%20the%20State%20of%20Alaska.&text=Finally%2C%20the%20bill%20will%20enable,businesses%20from%20selling%20that%20information
24. Google Stops Selling Ads: https://www.cnet.com/news/google-will-stop-selling-ads-based-on-tracked-individual-browsing-history/
25. Proposed CCPA-Like Legislation: https://www.jdsupra.com/legalnews/status-of-proposed-ccpa-like-state-8287625/#:~:text=House%20Bill%205959%20was%20introduced%20on%20February%2026%2C%202021.&text=The%20bill%20is%20limited%20to,Representative%20Capriglione%20introduced%20HB%203741.
26. Privacy Law Updates 2021: https://www.fastcompany.com/90606571/state-data-privacy-laws-2021
27. Sample DPIA Template: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf
28. Sample DPIA Template: https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx
29. ASC X9 PIA Standard & Templates: https://x9.org/
30. PIA/DPIA Checklist: https://www.colleaga.org/tools/data-protection-impact-assessment-dpia-template
31. GDPR: https://www.tessian.com/blog/biggest-gdpr-fines-2020/
32. CCPA: Privacy Enforcement Actions | State of California - Department of Justice - Office of the Attorney General

Connect with US

Reach out to the speakers to learn more about their background

Lisa McKee
Senior Manager, Protiviti
Security and Privacy
Lisa.McKee@Protiviti.com
Connect on LinkedIn

Michael Anderson
Senior Consultant, CompliancePoint
Security and Risk
Manderson@CompiancePoint.com
Connect on LinkedIn

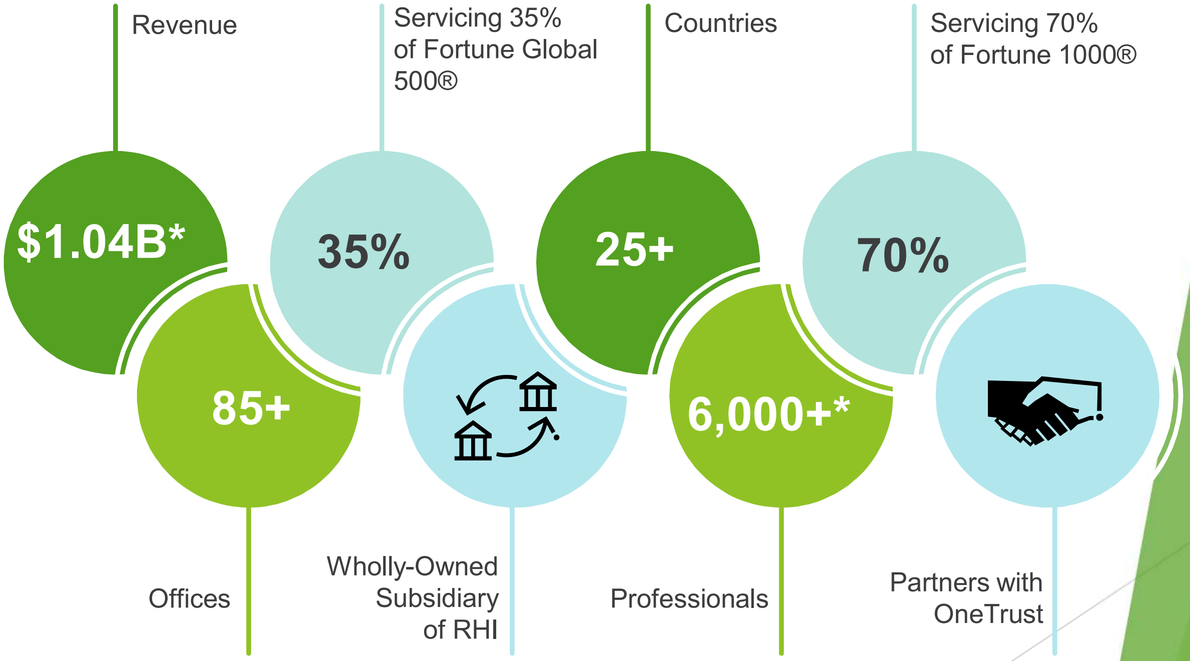
Thank You!

Reach out for a FREE Security or Privacy Workshop

- Security and Privacy Workshop Overview
  - Discuss organizational compliance obligations (CCPA/GDPR, PCI, FFIEC, etc.)
  - Overview of security and privacy laws and requirements and applicability to the organization
  - The current security and privacy program in place at the organization
  - Opportunities for to improve the current security and privacy posture
- Opportunities to strengthen the security and privacy programs across the organization
- Other areas that may need assistance outside security and privacy

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders face the future with confidence. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 85 offices in over 25 countries.



Revenue

$1.04B*

85+

Offices

Servicing 35% of Fortune Global 500®

35%

Wholly-Owned Subsidiary of RHI

Countries

25+

6,000+*

Professionals

Servicing 70% of Fortune 1000®

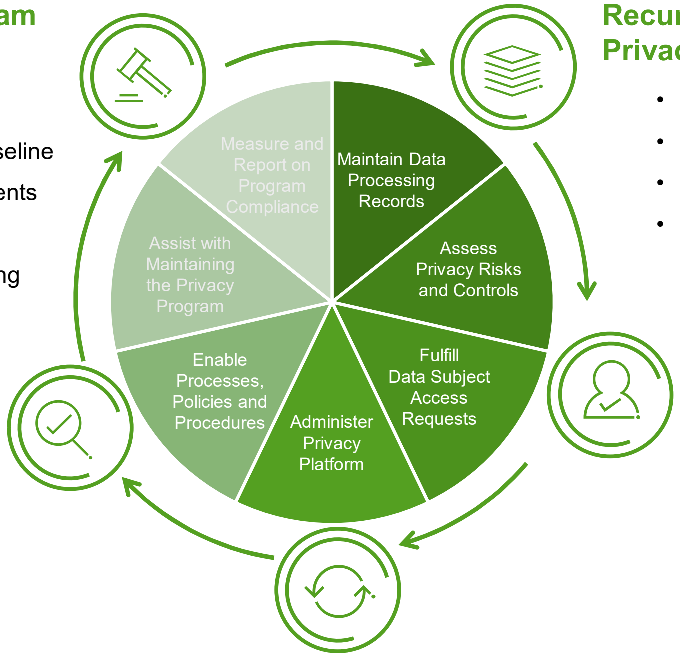
70%

Partners with OneTrust

Protiviti PRaaS Services

Privacy Legislation & Privacy Program Office Management

- Monitor Applicable Privacy Obligations
- Update Privacy Policies & Controls Baseline
- Conduct Annual Compliance Assessments
- Measure and Report Program Efficacy
- Conduct Annual Awareness and Training



Maintain Data Processing Records

Assess Privacy Risks and Controls

Fulfill Data Subject Access Requests

Administer Privacy Platform

Enable Processes, Policies and Procedures

Assist with Maintaining the Privacy Program

Measure and Report on Program Compliance

Recurring Data Inventory & Privacy Impact Assessments

- Maintain Inventory of Processing Activities
- Maintain Inventory of IT Systems and Data Classifications
- Perform Privacy Impact Assessments (PIAs)
- Perform Data Protection Impact Assessments (DPIAs)

Data Subject Rights (DSR) Request Management

- Manage Request Intake and Workflow Process
- Manage Access Request Fulfilment Process
- Manage Third-Party Request Fulfilment Process

Privacy By Design Engineering Support

- Provide privacy Subject Matter Experts (SMEs) to support Software Development Lifecycle (SDLC)
- Provide privacy SMEs to support requirements gathering, solution design and implementation efforts.

Privacy Platform Management

- Administer and Configure the OneTrust Environment