Internal Audit, Risk, Business & Technology Consulting

Data Privacy

Privacy Engineering, Privacy by Design & Privacy Shield Implications

LISA MCKEE & KATIE STEVENS

9/16/2020

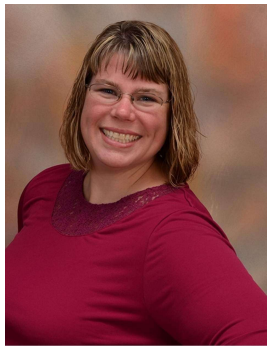
INNOVATE. TRANSFORM. SUCCEED

Adapt to the new business reality.

protiviti®

Face the Future with Confidence

TODAY'S SPEAKER



Lisa McKee,
CISA, CDPSE, PCIP

Senior Manager
Protiviti

protiviti®
Face the Future with Confidence

Katie Stevens

Director
Protiviti

TODAY'S TOPICS

- Data Privacy, Regulations and Consumer Rights
- Privacy Engineering & Privacy by Design
- Privacy Shield & Schrems II

POLLING QUESTION #1

What role best aligns with your job?

- a) Security/IT
- b) Privacy/Legal/Compliance
- c) Audit, Finance, HR
- d) Other

WHAT IS PRIVACY?

What is the difference between security and privacy?

Security refers to the systems and applications used to protect ourselves, our property and personal information. It is the first level of defense against unwanted intruders.

Privacy is protecting the data and our ability to control access to personal information.

Privacy Professional Resources - IAPP

IAPP - International Association of Privacy Professionals

- Certifications
  - Certified Information Privacy Professional (CIPP)
    - Asia (CIPP/A)
    - Canada (CIPP/C)
    - Europe (CIPP/E)
    - US Private Sector (CIPP/US)
  - Certified Information Technologist (CIPT)
  - Certified Information Privacy Manager (CIPM)
  - Certified Data Protection Officed (CDPO/F)
    - Requires CIPP/E
  - Privacy Law Specialist (PLS)
  - Fellow Information Privacy (FIP)

- KnowledgeNet Chapter Meetings
- Conferences
  - NIST Webinar for Privacy and Risk Management
  - https://iapp.org/store/conferences/a0l1P00000EXTYMQA5/
- Webinars
- Discounted Trainings
- Privacy Articles and Content
- Advisory Board Groups
- https://iapp.org/

IAPP Privacy Engineering
Advisory Board Member

Privacy Professional Resources - ISACA

ISACA – Information Systems Audit and Control

- Certifications
  - Certified Data Privacy Solutions Engineer

- Privacy in Practice Conference Dec 8th
  - https://www.isaca.org/conferences/isaca-virtual-conference-privacy-in-practice?cid=edmi_2005217&Appeal=EDMi&sp_rid=MTEwODY4MjgyNjM4S0&sp_mid=32507742&spMailingID=32507742&spUserID=MTEwODY4MjgyNjM4S0&spJobID=1783514659&spReportId=MTc4MzUxNDY1OQS2

- Webinars
- Discounted Trainings
- Privacy Articles and Content
- https://www.isaca.org/

POLLING QUESTION #2

Which privacy laws apply to your organization?

a) CCPA/USA Only

b) GDPR/Other International Areas

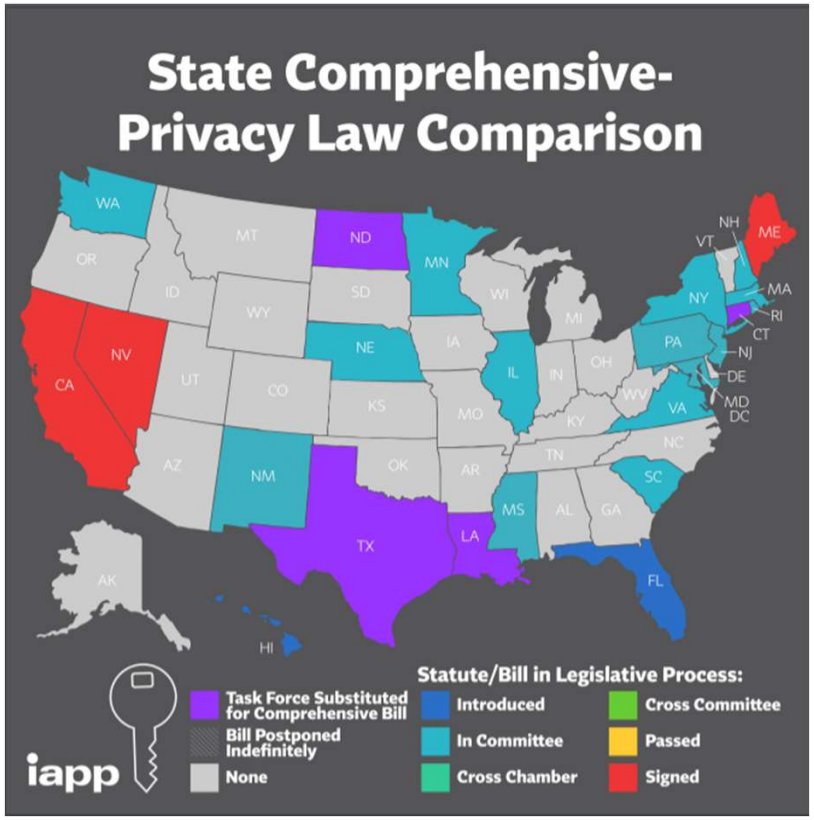
c) Both

d) None

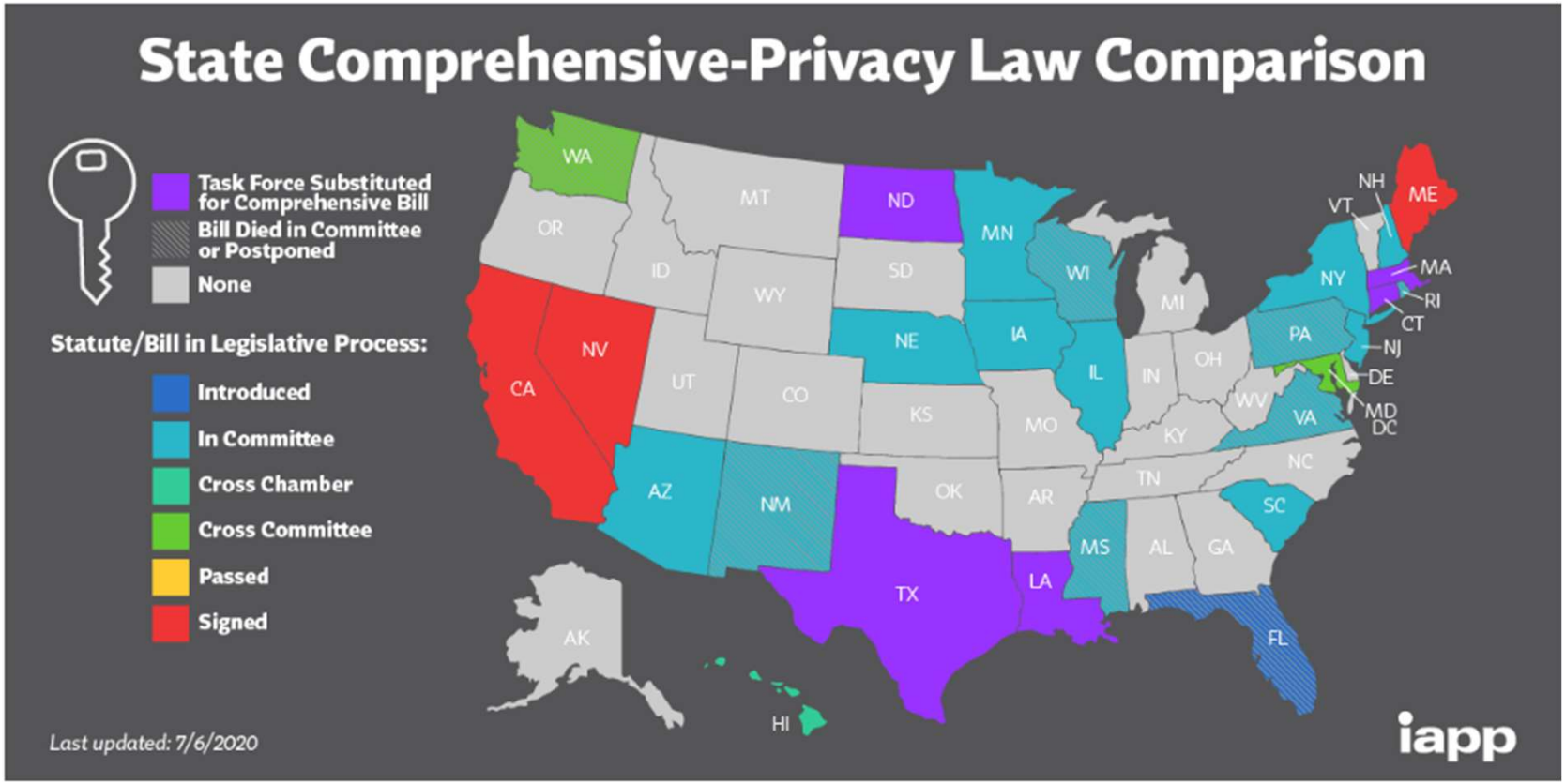
PRIVACY LAWS AND STANDARDS

- GDPR Regulation May 2018
- ISO Privacy Standard in 2019
- NIST Privacy Standard January 2020
- CCPA July 2020

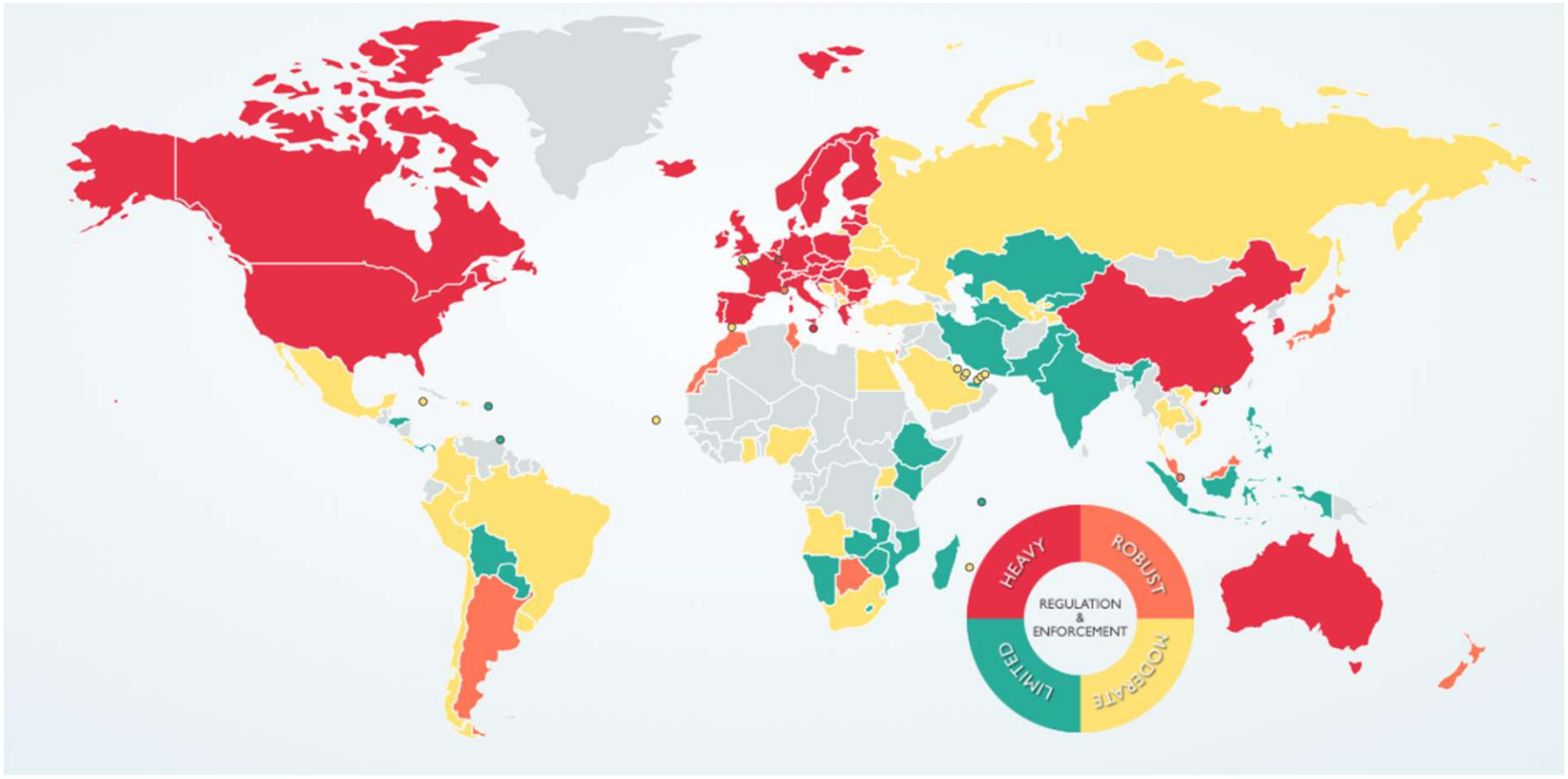
https://iapp.org/resources/article/state-comparison-table/#



PRIVACY LAWS ARE EVOLVING



GLOBAL PRIVACY LAWS



https://www.dlapiperdataprotection.com/

protiviti®

PRINCIPLES, STANDARDS AND FRAMEWORKS

Choosing the best one for your organization

Compliance

- General Data Protection Regulation(GDPR)
- International Standards Organization (ISO)
- ITIL (IT Infrastructure Library)
- National Institute of Standards and Technology (NIST)
- Sarbanes-Oxley Act (SOX)
- Frameworks
- COBIT 2019
- Health Insurance Portability and Accountability Act (HIPAA)
- SOX
- ANSI
- Federal Risk and Authorization Management Program (FedRAMp)

Privacy

- Fair Information Practices (FIPs)
- Organization for Economic Co-operation and Development (OECD)
- Generally Accepted Privacy Principles (GAPP)
- Canadian Standards Association Privacy Code
- Asia-Pacific Privacy Framework
- Binding Corporate Rules (BCRs)
- ETSI Standards
- International Standards Organization (ISO)
- NIST
- ANSI
- X9
- COBIT 2019

Security

- PCI Data Security Standards
- COBIT 2019
- COSO
- HITRUST
- NERC/CIP
- NIST
- ISO/IEC
- SANS
- CERT
- ANSI
- Information Security Manual

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

CORE PRIVACY RIGHTS

Access

- Free access to personal information that is collected on the consumer.
- Includes providing who else has access to the information.
- Must be prompt
  - GDPR 30 days
  - CCPA 45 days
  - LGPD 15 Days

Disclosure

- Provide privacy and data collection policies at or before time of collection.
- Disclose purpose of the information collection.
- Inform consumers of their rights under GDPR / CCPA.

Opt Out

- Consent must be obtained to market to the consumer (GDPR).
- Consumer can object to automated processing of data (GDPR).
- Consumer can opt out of having their information sold or transferred to other businesses or third parties (CCPA).

Deletion

- With certain exceptions, consumers have the right to have information about them deleted.
  - All data concerning the subject (GDPR).
  - All data collected from the consumer (CCPA).

GDPR VS. CCPA REQUIREMENTS

1. Data Protection Officer
Evaluate privacy and data protection governance structure and the need for a Data Protection Officer (DPO).

2. Legal Basis for Processing
Evaluate the legal basis on which personal data is collected and processed.

3. Privacy Notice & Disclosures
Evaluate external privacy notice and disclosures as well as internal policies and employee training procedures.

4. Consent Management
Evaluate consent practices, when relying on individual's consent for processing personal data.

5. Individual Privacy Rights
Evaluate processes that address the rights of individuals (e.g., access, rectification, erasure, and portability of personal data).

6. Privacy Impact Analysis
Evaluate data collection and usage practices to determine if a Data Protection Impact Assessment (DPIA) is required.

7. Records of Processing
Evaluate records of processing activities and data inventories as well as the process to maintain such records.

8. Cross-Border Data Transfer
Evaluate the legitimate mechanisms for transferring personal data outside of the defined territory.

9. Third-Party Management
Evaluate contractual agreements and control validation procedures for third-party vendors with whom personal data is shared.

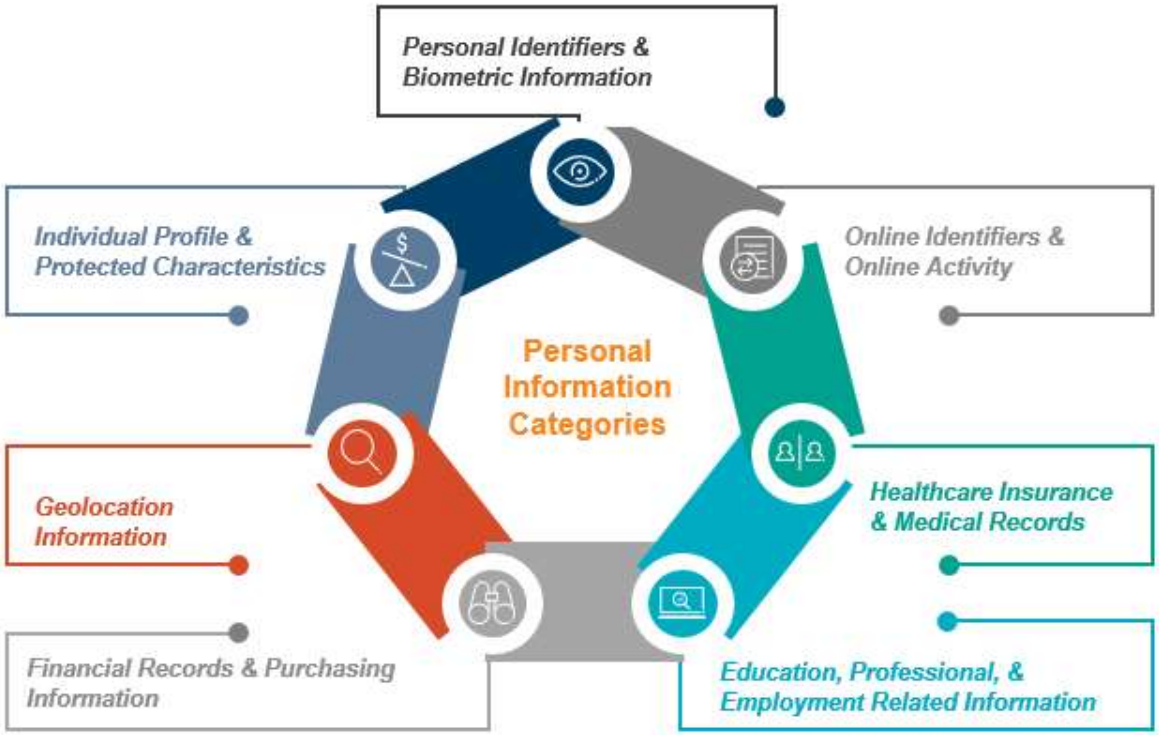
10. Privacy by Design & Default
Evaluate data minimization and retention practices; validate that privacy safeguards are considered prior to new implementations.

11. Data Security
Evaluate data security controls employed to help ensure confidentiality, availability and integrity of personal data.

12. Brach Notification
Evaluate the Incident Response procedures and the breach notification process.

Privacy Law: ● General Data Protection Regulation (GDPR) ● California Consumer Privacy Act (CCPA) & Civil Code

PERSONAL INFORMATION CATEGORIES



protiviti

Data Protection Roles

What Role is Your Company?

- Data Subject
  - Individual whom information is being collected and/or processed
- Data Controller
  - Organization or individual with the authority to decide how and why personal data about data subject is to be processed
  - Perform any operation upon personal data
- Data Processor
  - Organization or individual that processes data on behalf of the data controller
  - NOTE: a processor that determines the purposes and means of the processing may be a controller
- Supervisory Authority
  - Supervisory entity chartered to enforce privacy or data protection laws and regulations

POLLING QUESTION #3

What stage is your organization in adopting privacy engineering and privacy by design?

- a) No Program
- b) Initial Stages
- c) Progressively Improving
- d) Holistic, Robust Program

PRIVACY ENGINEERING

HOW TO GET STARTED IN PRIVACY ENGINEERING

1 Pursue a cross-disciplinary education.

- If you are still in college or exploring higher-ed options, seek a degree in privacy engineering, computer science, software/computer engineering, networking, information systems, data science or analytics, cybersecurity, or other technical field, and take courses that focus on privacy.
- Look for opportunities to take data protection-related courses across schools or pursue continuing education online, in areas such as cybersecurity, user testing, risk management, law, and UX or UI design.
- Practice privacy skills through an internship or externship with a local company, government privacy office, think tank or civil rights advocacy organization. Learn how to work with technical, legal and business professionals.

2 Search for career opportunities beyond Big Tech.

- Don't limit yourself as to where you might work or what your title might be. Nearly all companies and industries today require technology and data skills. Consider positions where privacy engineering is a component of the role that could grow, whether in more traditional companies that are expanding their digital presence, newer startups or as part of larger teams within more recognizable tech companies.
- Consider post-graduate fellowships in organizations with a privacy focus, such as the IAPP, Future of Privacy Forum and academic research centers, such as Berkman Klein Center for Internet & Society at Harvard University.
- Explore privacy careers listed on the IAPP's Career Central page.

4 Network, network, network: Engage with privacy professionals.

- Become a member of the IAPP and join the Privacy Engineering Section.
- Attend virtual and, when possible, in-person privacy conferences, IAPP privacy engineering forums, PEPR, PETS, SOUPS and others, KnowledgeNet Chapter meetings, and after hours events. Some conferences provide scholarships for students. Or pitch a session for a speaker pass.
- Reach out to privacy professionals in your community, and arrange to meet for coffee.
- Seek out opensource initiatives that focus on solving data and privacy problems to learn tech practices.
- Subscribe to a privacy email list, such as the IAPP Privacy List.

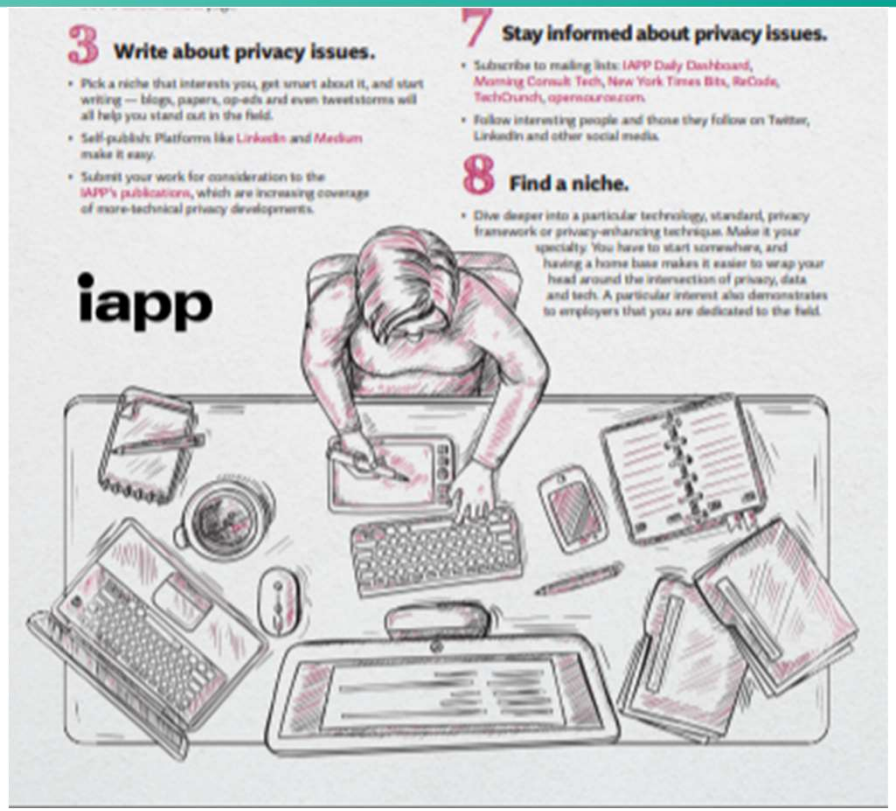
5 Become an expert in your own privacy.

- Learn to follow your data. Understand where it goes and who controls it.
- Manage your own privacy with mobile device settings, encryption, location tracking, etcetera.

6 Earn privacy credentials.

- Become a Certified Information Privacy Technologist.
- Earn privacy-related continuing education credits through conferences, trainings, etcetera.

ttps://iapp.org/resources/article/infographic-how-to-get-started-in-privacy-engineering
https://iapp.org/connect/join-privacy-engineering-section-advisory-board//



3 Write about privacy issues.

- Pick a niche that interests you, get smart about it, and start writing — blogs, papers, op-eds and even tweetstorms will all help you stand out in the field.
- Self-publish: Platforms like LinkedIn and Medium make it easy.
- Submit your work for consideration to the IAPP's publications, which are increasing coverage of more-technical privacy developments.

7 Stay informed about privacy issues.

- Subscribe to mailing lists: IAPP Daily Dashboard, Morning Consult Tech, New York Times Bits, ReCode, TechCrunch, opensource.com.
- Follow interesting people and those they follow on Twitter, LinkedIn and other social media.

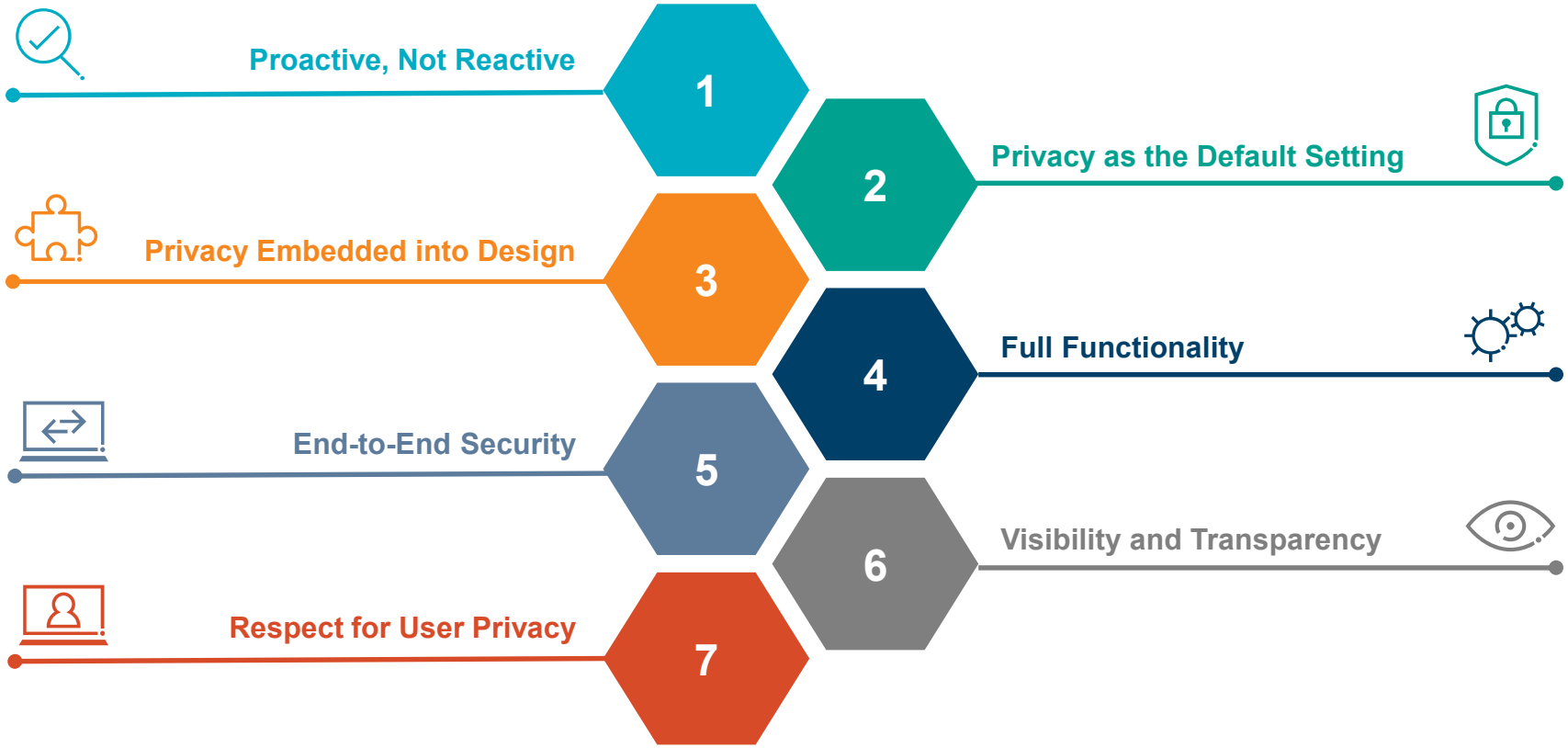
8 Find a niche.

- Dive deeper into a particular technology, standard, privacy framework or privacy-enhancing technique. Make it your specialty. You have to start somewhere, and having a home base makes it easier to wrap your head around the intersection of privacy, data and tech. A particular interest also demonstrates to employers that you are dedicated to the field.

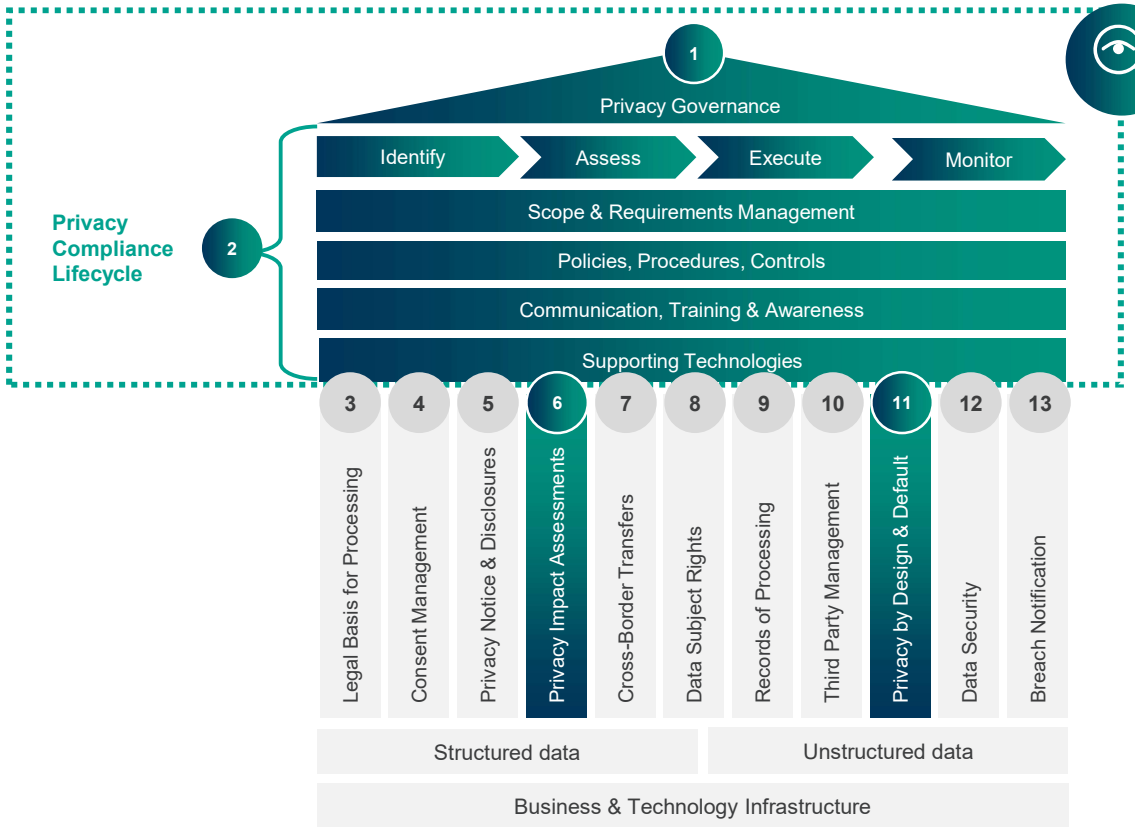
iapp

https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering

PRIVACY BY DESIGN – CORE PRINCIPLES



EMBEDDING IN YOUR PRIVACY PROGRAM



Governance & Change Management

- Define Roles & Responsibilities for identifying and assessing changes
- Establish standards and assessment templates

Privacy Impact Assessment Process

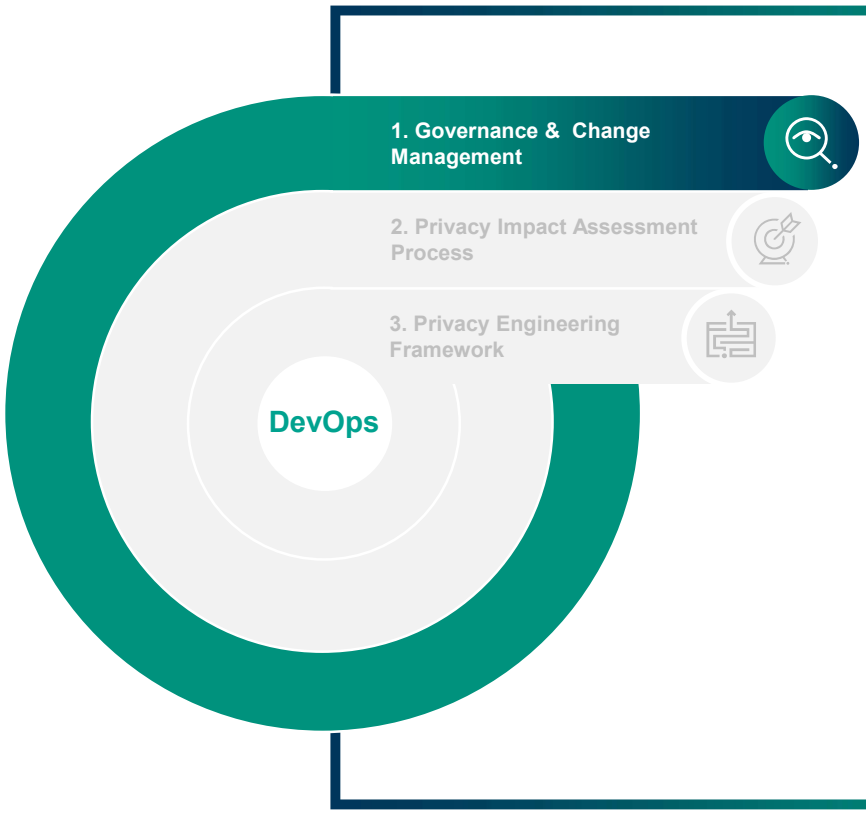
- Implement a Privacy Impact Assessment (PIA) process and procedures
- Establish a standard Data Protection Impact Assessment (DPIA) template
- Conduct PIAs and DPIAs for new and updated technologies

Privacy Engineering Framework

- Privacy Embedded in your Software Development Lifecycle (SDLC)
- Engineer new and updated technologies with appropriate privacy controls.
- Implement privacy compliant solutions.

protiviti®

UNDERSTANDING YOUR ENVIRONMENT



- Key Roles & Responsibilities
- Standards & Templates

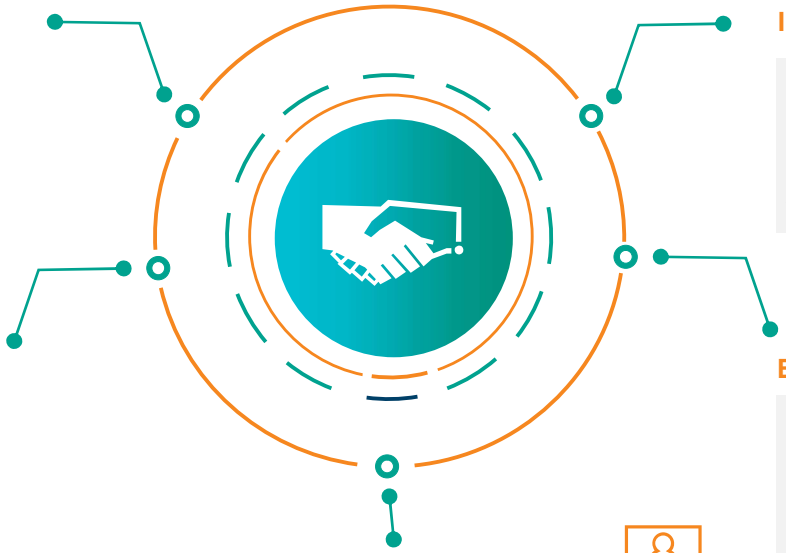
KEY ROLES & RESPONSIBILITIES

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.

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.



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.

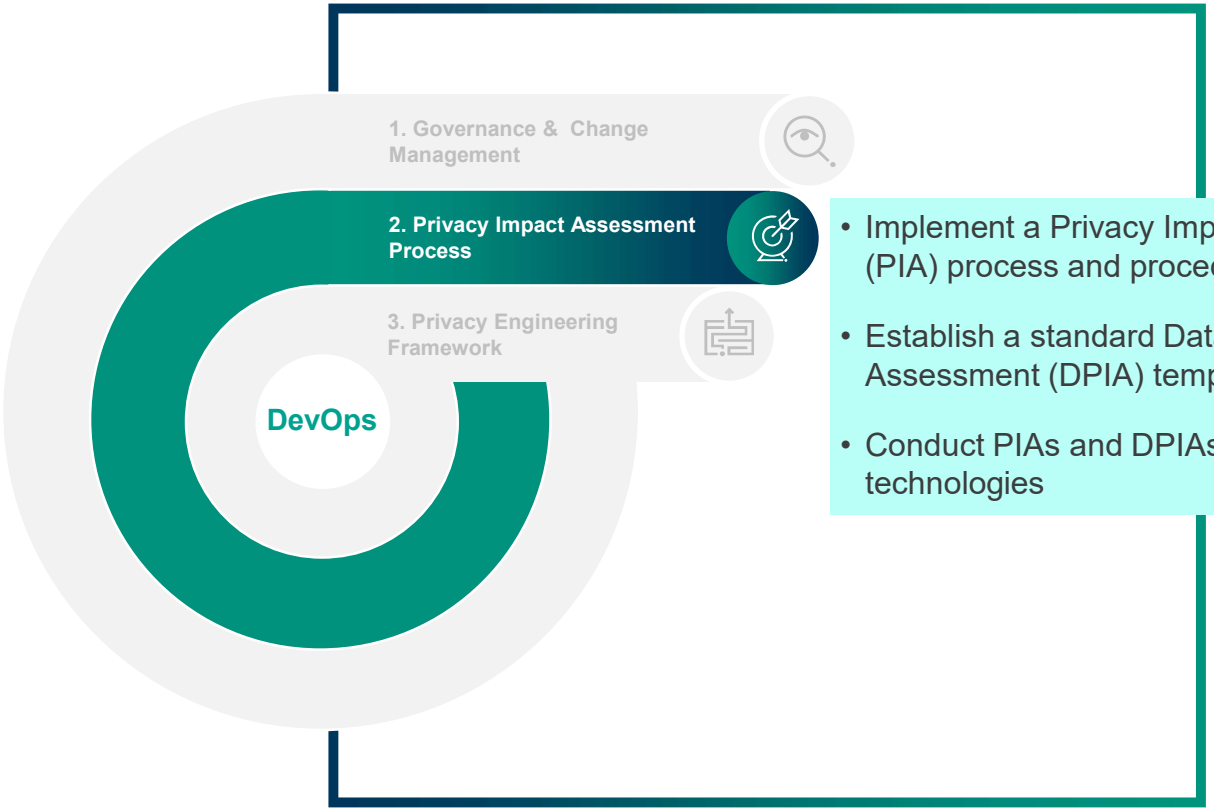
Business Stakeholders

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.

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).

EMBEDDING PRIVACY IN YOUR ORGANIZATION

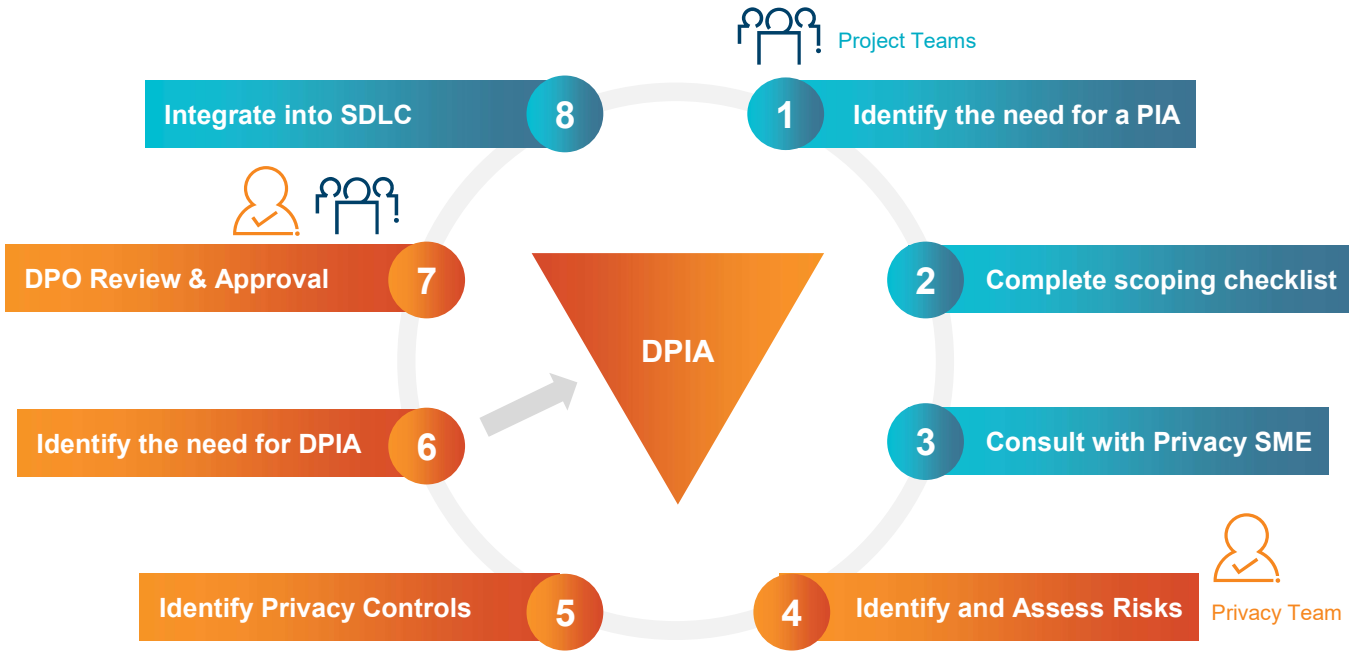


- Implement a Privacy Impact Assessment (PIA) process and procedures
- Establish a standard Data Protection Impact Assessment (DPIA) template
- Conduct PIAs and DPIAs for new and updated technologies

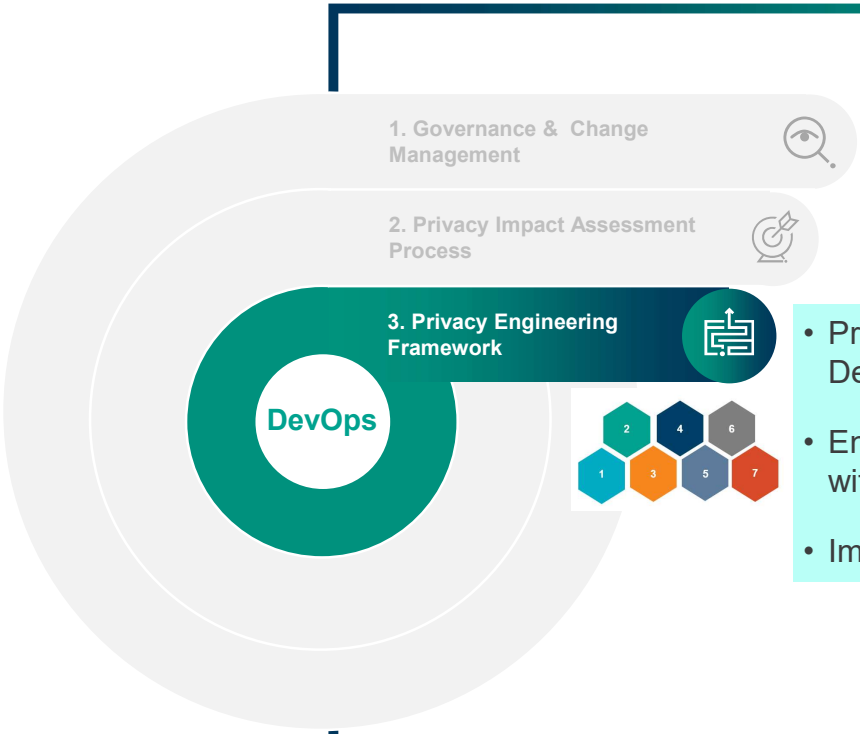
protiviti®

PRIVACY IMPACT ASSESSMENT 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.



PRIVACY BY DESIGN FOR DEVELOPMENT



- Privacy Embedded in your Software Development Lifecycle (SDLC)
- Engineer new and updated technologies with appropriate privacy controls.
- Implement privacy compliant solutions.

protiviti®

SDLC – OVERVIEW

Privacy Requirements Definition

Privacy Strategy Selection & Design

Privacy Controls Validation

Initiation of Data Processing

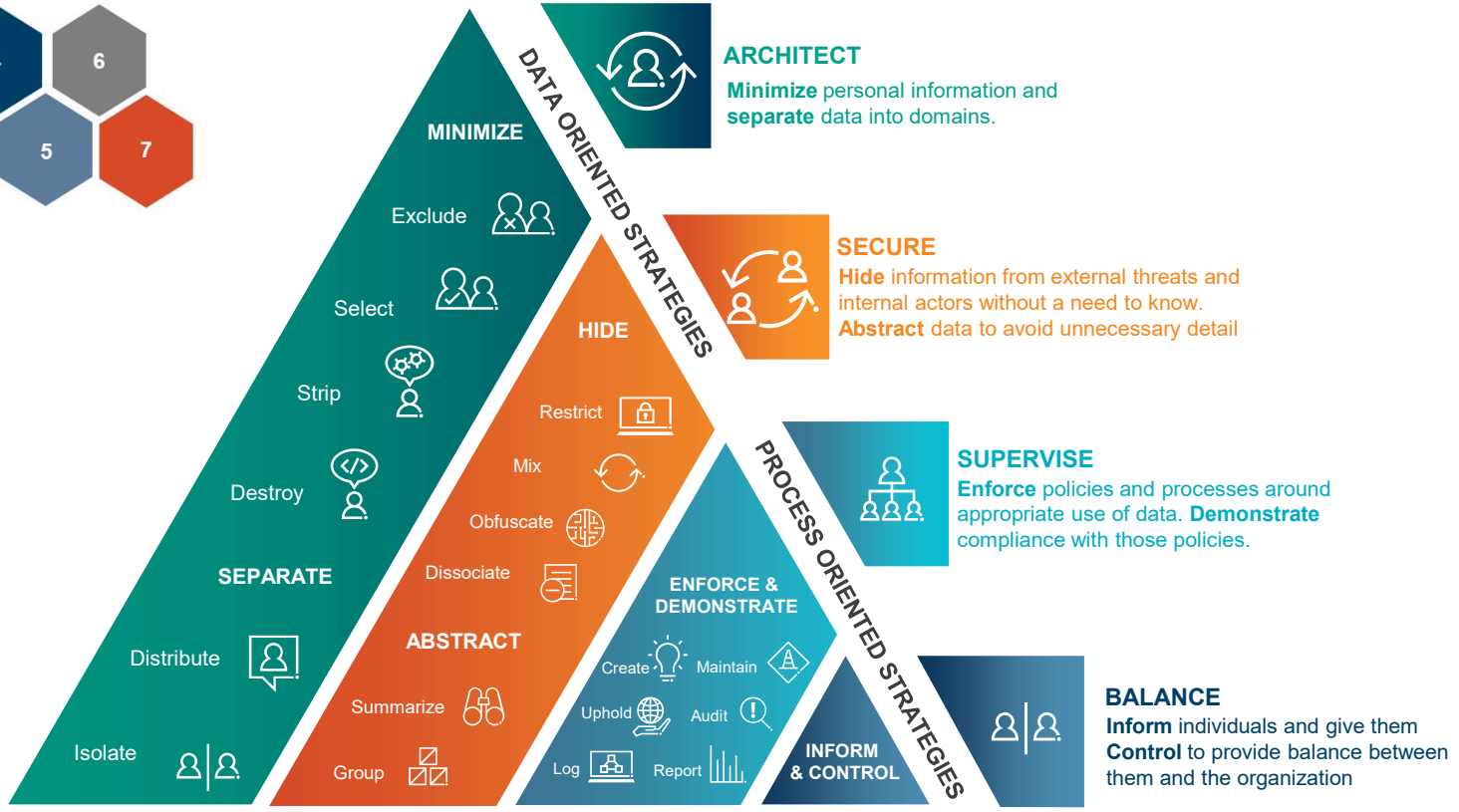
Secure Data Disposal

Privacy Control Gates

SDLC Phases

Initiation	Design & Development	Implementation & Assessment	Operation & Maintenance	Disposal
• Defining the scope and conducting initial Privacy Impact Analysis (PIA) • Key activities are: – Delineate business requirements – Determine information categorization and data subject impact – Determine privacy requirements	• Key activities include: – Develop privacy specific user stories – Design security and privacy architecture – Perform functional and testing; – Prepare documents for system verification; – Conduct a Data Protection Impact Assessment (DPI) is necessary.	• It includes system installation and evaluation in organization's environment. • Key activities are: – Integrate information system; – Plan system certification and security controls testing activities; – Conduct system accreditation.	• It includes operating systems, tested enhancements, and hardware/software replacement. • Key activities include: – Conduct operational readiness review; – Manage system configuration; – Monitor information system's controls; – Perform reauthorization.	• It provides system disposal, information archival, and contracts closeout. • Key activities include: – Build and execute disposal plan; – Archive critical information; – Sanitize media; – Dispose hardware and software.

PRIVACY DESIGN STRATEGIES



ARCHITECT
Minimize personal information and **separate** data into domains.

SECURE
Hide information from external threats and internal actors without a need to know. **Abstract** data to avoid unnecessary detail

SUPERVISE
Enforce policies and processes around appropriate use of data. **Demonstrate** compliance with those policies.

BALANCE
Inform individuals and give them **Control** to provide balance between them and the organization

protiviti®

PRIVACY RISKS

What is the data and what does the organization do with it?

1. Overcollection of data – collecting data beyond what is necessary for processing
2. Usage of data outside of the reason it was collected or captured without consent
3. Undefined retention standards – holding data beyond a reasonable time frame
4. Lack of defined policies and procedures – right to erasure requests
5. Knowing your compliance landscape – what countries does your company do business

DATA MANAGEMENT CHALLENGES

- When good data governance is not present, multi-system mapping exercises required.
- Cryptography and other obfuscation or anonymization routines must be implemented.
- Multi-disciplinary expert-level technical resources needed.

- In most cases, manual processing will be required for a period of time.
- High volumes of requests can create performance challenges for OLTP systems.
- Additional work required around data retention, governance and other processes to keep up with changes.

- What data can be kept as part of valid business operations.
- Where is encryption, anonymization or pseudonymization appropriate.
- When is deletion or segregation of records or fields required as part of complying with existing laws.

POLLING QUESTION #4

Was your organization impacted by the fallout from Privacy Shield and the Schrems II decision?

a) Yes

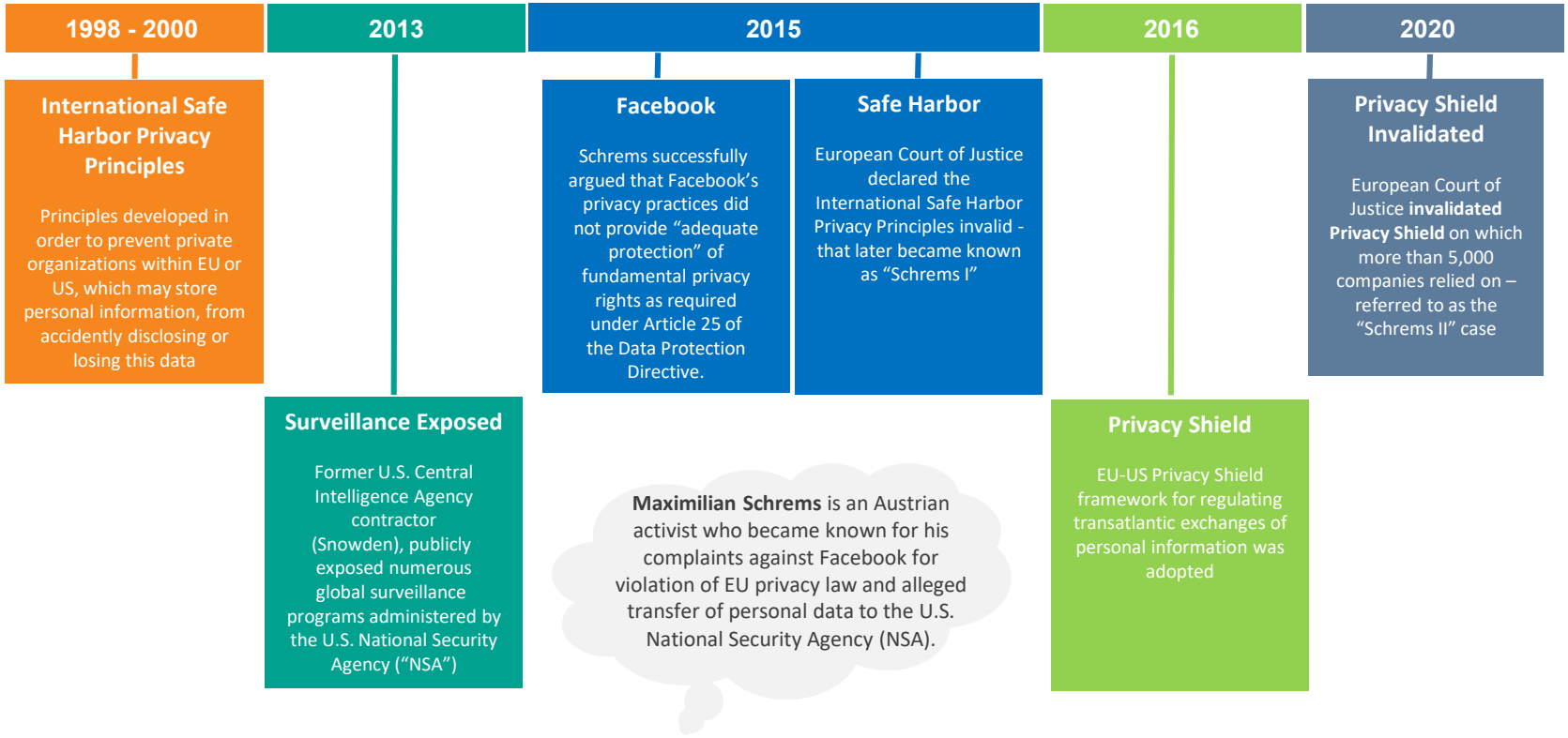
b) No

c) Unsure

d) Other

HISTORY OF CROSS-BORDER DATA TRANSFERS

innovate



protiviti®

OVERVIEW OF SCHREMS II DECISION AND PRIVACY SHIELD

U.S. companies that have relied on their EU-US Privacy Shield certifications can no longer use Privacy Shield as their mechanism for data transfers of personal information from the EU to the U.S.

What does the invalidation mean for US businesses with EU interests?

- Organizations using Standard Contractual Clauses (SCCs) or Binding Corporate Rules to transfer personal data must ***assess if they need to implement supplementary measures***
- Data controllers should examine the data protection laws of the receiving country to ***determine whether adequate protections are in place*** and align to the EU General Data Protection Regulation (GDPR) and Member State legal requirements
- Controllers should ***assess the likelihood that their processors(s) may share personal data*** with public authorities
- Data Protection Officers (DPOs) and other controllers should ***make risk-informed decisions on a case-by case basis*** to protect the privacy rights of EU residents
- Where appropriate safeguards would not be ensured during data transfer, organizations are ***required to suspend transfers of personal data or notify the relevant supervisory authority*** that it wishes to continue transferring data.

Challenges:

- Incomplete view of country-to-country transfers
- Incomplete view of how and where third parties are transferring information
- Incomplete view of FISA 702 implications and national laws that contradict GDPR requirements
- Insufficient resources & lengthy timeline to implement alternative legal instruments
- No grace period

Consequences:

- EU Controllers and Data Protection Authorities (DPAs) have a duty to suspend or prohibit data transfers when they lack a valid legal instrument for a transfer
- GDPR penalty of € 20M or 4% of the global turnover if the organization continues to transfer data without a valid legal instrument

HOW CAN YOU PREPARE?

transform

1. Convene the privacy and data governance teams to understand the impact of the ruling and set a new strategic course on EU-US data transfers.
2. Conduct an analysis to understand where *Privacy Shield* requirements have been in use, with specific emphasis on vendor relationships.
3. Review all data export / import arrangements and storage locations and determine the legal instruments in place.
4. Review SCCs for 3rd countries to ensure adequacy of protection on a case-by-case basis ensuring stringent data protections considering the Schrems II decision. For example, implementing Binding Corporate Rules – although this may present similar issues and a longer timeframe.
5. Revisit contractual terms with third parties regarding data transfers and identify FISA 702 concerns for any electronic communications providers; identify national laws that contradict expectations of GDPR.
6. Review the organization's privacy policies and public notices. Consult with legal counsel to update documents to reflect compliant terms.
7. Review your current operational privacy practices, as applicable.

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 to strengthen the security and privacy programs across the organization
- Other areas that may need assistance outside security and privacy

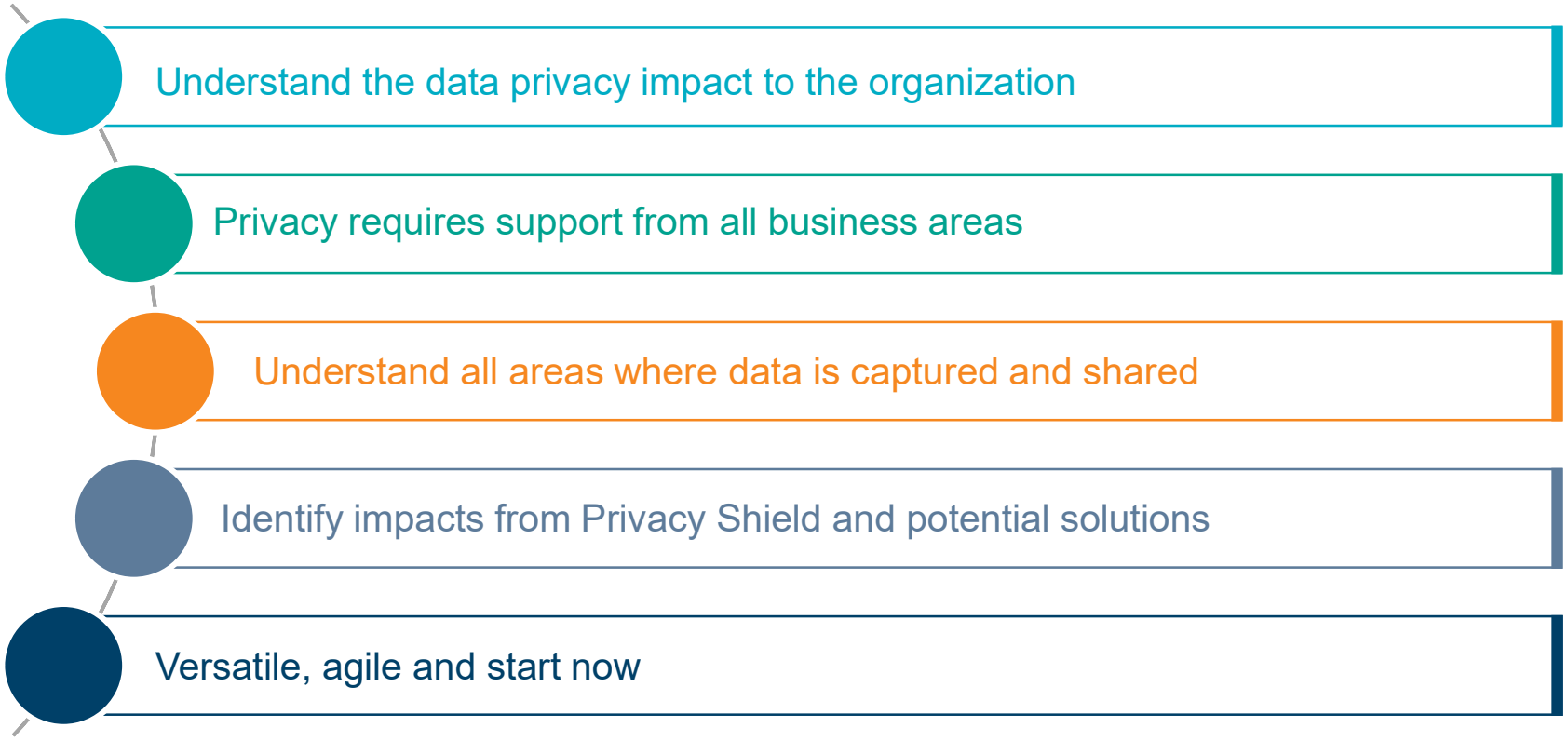
POLLING QUESTION #5

Would you be interested in a free privacy workshop?

a) Yes

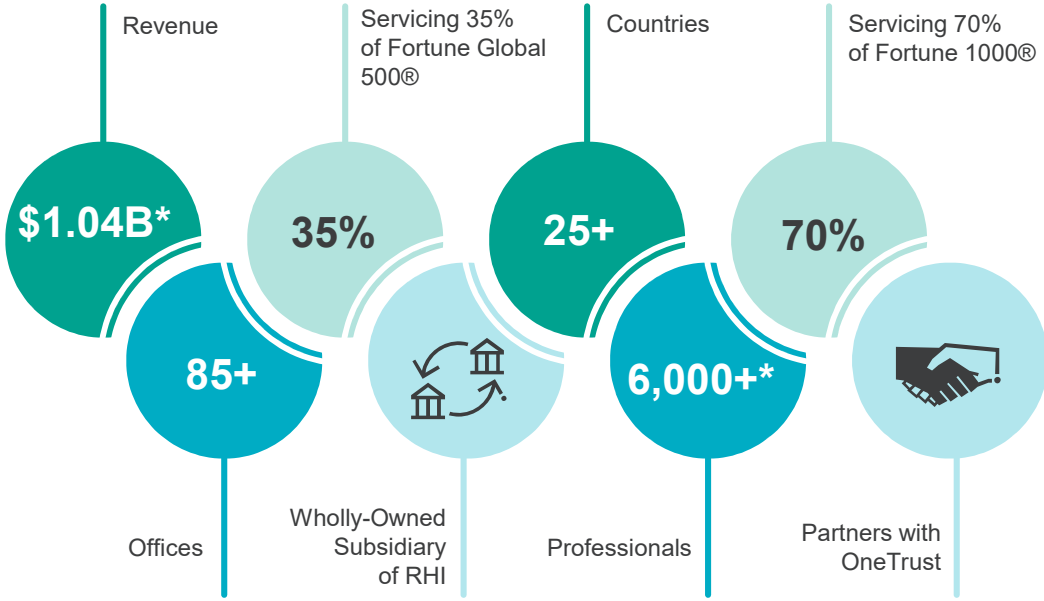
b) No

FINAL THOUGHTS



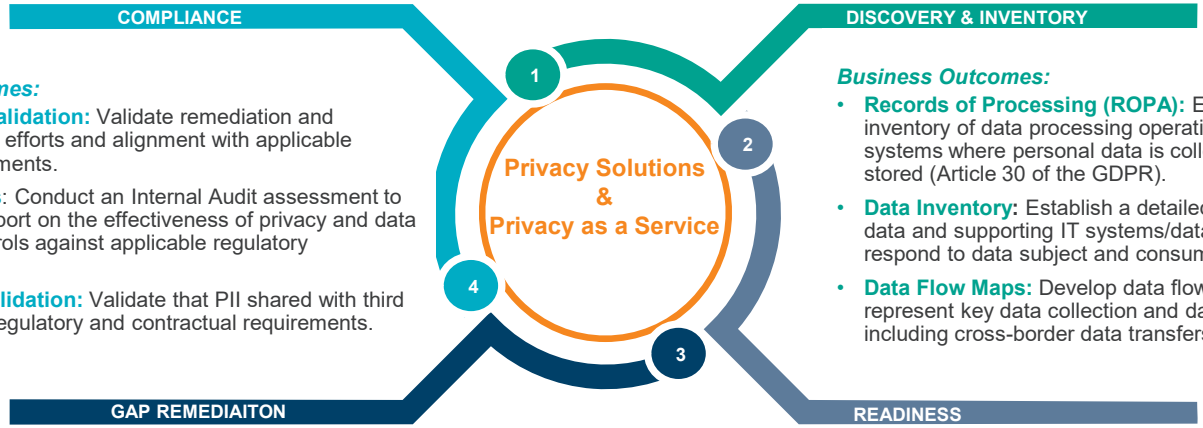
ABOUT PROTIVITI

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.



protiviti®

OVERVIEW OF PRIVACY SERVICES



Business Outcomes:

- **Compliance Validation:** Validate remediation and implementation efforts and alignment with applicable privacy requirements.
- **Privacy Audits**: Conduct an Internal Audit assessment to validate and report on the effectiveness of privacy and data protection controls against applicable regulatory requirements.
- **Third-Party Validation:** Validate that PII shared with third parties meets regulatory and contractual requirements.

Business Outcomes:

- **Records of Processing (ROPA):** Establish a formal inventory of data processing operations and supporting systems where personal data is collected, processed, and stored (Article 30 of the GDPR).
- **Data Inventory:** Establish a detailed inventory of personal data and supporting IT systems/data stores to effectively respond to data subject and consumer requests.
- **Data Flow Maps:** Develop data flow diagrams to visually represent key data collection and data transmission points, including cross-border data transfers.

Business Outcomes:

Design and implement privacy and data protection solutions, including the following key areas:

- Privacy Program & Governance Structure
- Consent & Cookie Management
- Privacy Notifications & Privacy Shield (RHL)
- Privacy Impact Assessments
- Data Subject Rights
- Third-Party Risk Management
- Privacy by Design & Default
- Data Security & Breach Notification

Our Software Partners:

OneTrust Privacy Management Software

SPIRION

BigID

Prevalent

Informatica

Business Outcomes:

- **Privacy Obligations:** Establish a formal baseline and scope of privacy obligations based on applicable privacy regulations, including GDPR, CCPA, HIPAA, PIPEDA, etc.
- **Privacy & Data Protection Roadmap:** Identify gaps and develop a formal Privacy and Data Protection strategy and roadmap to meet privacy obligations
- **Third-Party Contract Review:** Evaluate and redline contractual agreements with third-party processors (RHL).

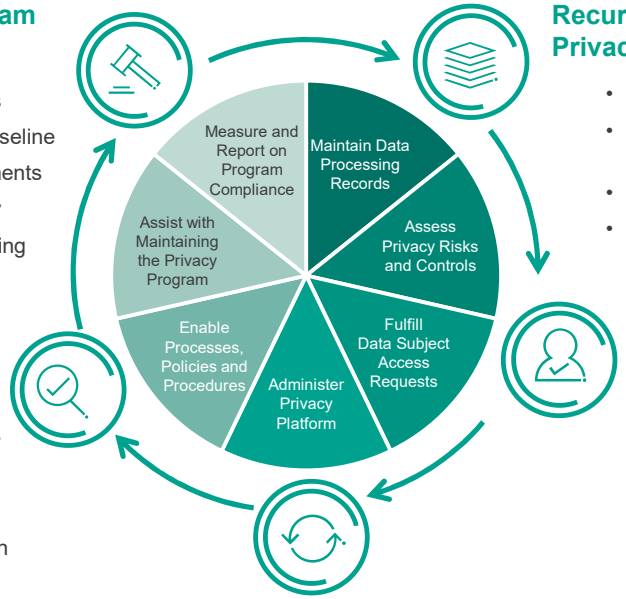
PROTIVITI PRAAS SERVICES

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

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.



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 Platform Management

- Administer and Configure the OneTrust Environment

TECHNOLOGY CONSULTING - SOLUTION OVERVIEW

Technology Strategy and Operations
- Technology Strategy and Architecture
- Technology Governance and Risk Management
- Transformation Program Execution
- Technology Operations and Delivery

Enterprise Application Solutions
- Solution Design and Selection
- Implementation Support
- Application Security and Controls
- Point Solution Implementation

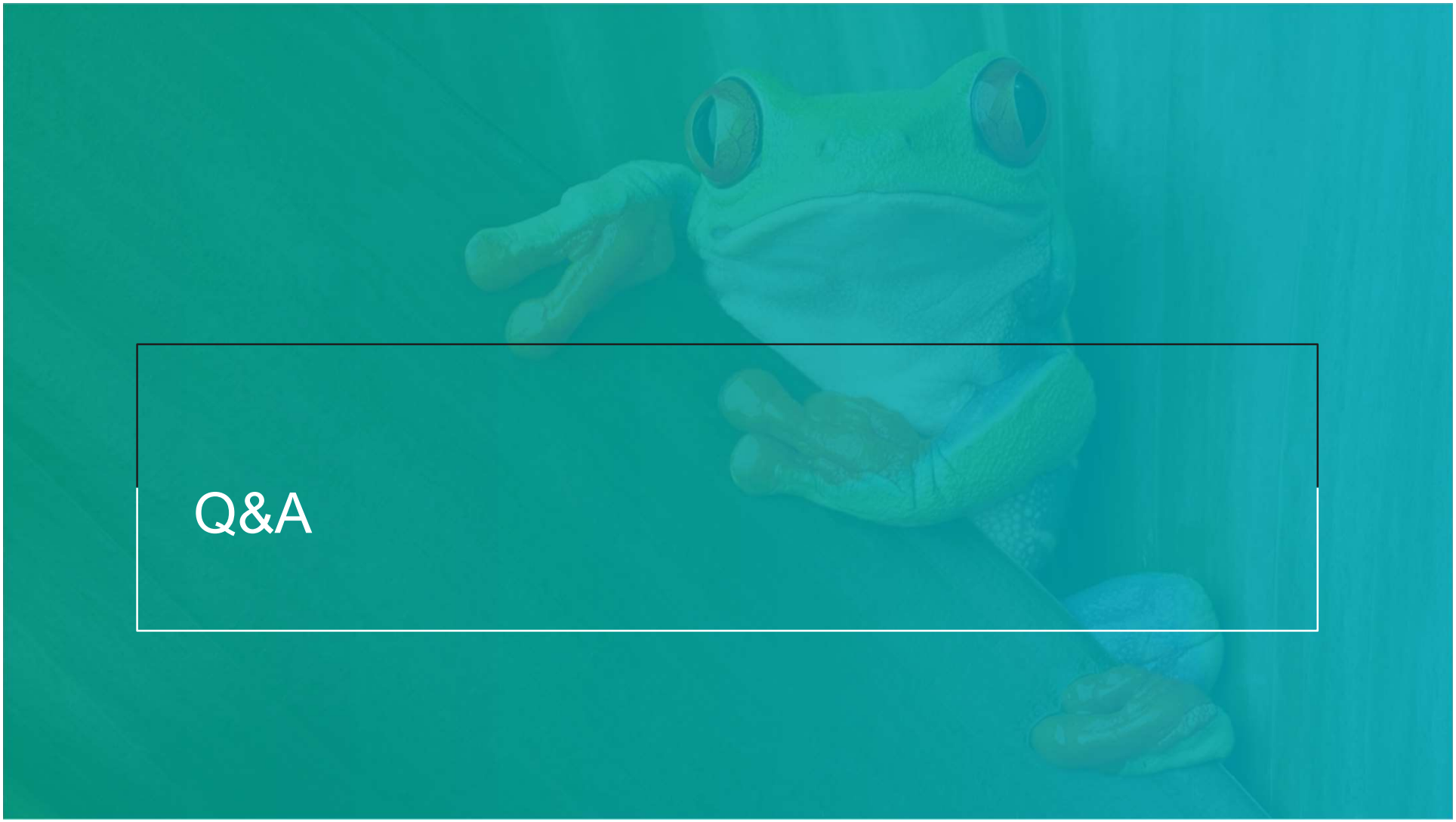
Security and Privacy
- Security and Privacy Program and Strategy
- Cyber Security Operations and Implementation
- Digital Identity and Access Management
- Technical Security and Data Security and Privacy
- Incident Response, Forensics and Recovery

Software Services
- Custom Business Applications
- Cloud, Portals and Collaboration
- Website Design and Solutions
- Intelligent Automation Enablement
- On-Demand Services and GRC Solution Implementation

Cloud Solutions
- Cloud Strategy and Architecture
- Cloud Applications
- Cloud Modernization
- Cloud Security

Enterprise Data and Analytics
- Enterprise Data Governance
- Enterprise Information Management
- Reporting and Visualization
- Digital Transformation and Software Services
- Business Strategy and Advanced Analytics

protiviti


Q&A

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

Katie Stevens
Director, Protiviti
Security and Privacy
Katie.Stevens@Protiviti.com
Connect on LinkedIn

Face the Future with Confidence

protiviti®