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.
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
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 Officer (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](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/](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/#
State Comprehensive-Privacy Law Comparison

- **Task Force Substituted for Comprehensive Bill**: Purple
- **Bill Died in Committee or Postponed**: Gray
- **None**: White

**Statute/Bill in Legislative Process:**
- **Introduced**: Red
- **In Committee**: Teal
- **Cross Chamber**: Light Blue
- **Cross Committee**: Turquoise
- **Passed**: Purple
- **Signed**: Black

*Last updated: 7/6/2020*
GLOBAL PRIVACY LAWS

https://www.dlapiperdataprotection.com/
### PRINCIPLES, STANDARDS AND FRAMEWORKS

Choosing the best one for your organization

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>- General Data Protection Regulation (GDPR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- International Standards Organization (ISO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ITIL (IT Infrastructure Library)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- National Institute of Standards and Technology (NIST)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Sarbanes-Oxley Act (SOX)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Frameworks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- COBIT 2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Health Insurance Portability and Accountability Act (HIPAA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- SOX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Federal Risk and Authorization Management Program (FedRAMp)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Fair Information Practices (FIPs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Organization for Economic Co-operation and Development (OECD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Generally Accepted Privacy Principles (GAPP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Canadian Standards Association Privacy Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Asia-Pacific Privacy Framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Binding Corporate Rules (BCRs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ETSI Standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- International Standards Organization (ISO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- X9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- COBIT 2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- PCI Data Security Standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- COBIT 2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- COSO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- HITRUST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- NERC/CIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ISO/IEC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- SANS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- CERT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Information Security Manual</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Privacy Law: General Data Protection Regulation (GDPR)</th>
<th>California Consumer Privacy Act (CCPA) &amp; Civil Code</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>1. Data Protection Officer</strong></th>
<th>Evaluate privacy and data protection governance structure and the need for a Data Protection Officer (DPO).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2. Legal Basis for Processing</strong></td>
<td>Evaluate the legal basis on which personal data is collected and processed.</td>
</tr>
<tr>
<td><strong>3. Privacy Notice &amp; Disclosures</strong></td>
<td>Evaluate external privacy notice and disclosures as well as internal policies and employee training procedures.</td>
</tr>
<tr>
<td><strong>4. Consent Management</strong></td>
<td>Evaluate consent practices, when relying on individual’s consent for processing personal data.</td>
</tr>
<tr>
<td><strong>5. Individual Privacy Rights</strong></td>
<td>Evaluate processes that address the rights of individuals (e.g., access, rectification, erasure, and portability of personal data).</td>
</tr>
<tr>
<td><strong>6. Privacy Impact Analysis</strong></td>
<td>Evaluate data collection and usage practices to determine if a Data Protection Impact Assessment (DPIA) is required.</td>
</tr>
<tr>
<td><strong>7. Records of Processing</strong></td>
<td>Evaluate records of processing activities and data inventories as well as the process to maintain such records.</td>
</tr>
<tr>
<td><strong>8. Cross-Border Data Transfer</strong></td>
<td>Evaluate the legitimate mechanisms for transferring personal data outside of the defined territory.</td>
</tr>
<tr>
<td><strong>9. Third-Party Management</strong></td>
<td>Evaluate contractual agreements and control validation procedures for third-party vendors with whom personal data is shared.</td>
</tr>
<tr>
<td><strong>10. Privacy by Design &amp; Default</strong></td>
<td>Evaluate data minimization and retention practices; validate that privacy safeguards are considered prior to new implementations.</td>
</tr>
<tr>
<td><strong>11. Data Security</strong></td>
<td>Evaluate data security controls employed to help ensure confidentiality, availability and integrity of personal data.</td>
</tr>
<tr>
<td><strong>12. Brach Notification</strong></td>
<td>Evaluate the Incident Response procedures and the breach notification process.</td>
</tr>
</tbody>
</table>

© 2020 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
1. Any Information
   - Collected or meant to be collected
2. Relating To
   - Relationship by content (name, job title, address)
   - Purpose
   - Impact on someone's privacy rights
3. An Identified or Identifiable
   - Name or singling out
   - Specific characteristics
4. Natural Person
   - Indirect

   - Are they living, can you in any way Google, search or otherwise, find that person with the data you have?
   - Note: some countries extend personal data protection to corporate data (ie Austria) as well as deceased persons.

---

**PERSONAL INFORMATION CATEGORIES**

- Personal Identifiers & Biometric Information
- Individual Profile & Protected Characteristics
- Online Identifiers & Online Activity
- Geolocation Information
- Healthcare Insurance & Medical Records
- Financial Records & Purchasing Information
- Education, Professional, & Employment Related Information
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 BY DESIGN – CORE PRINCIPLES

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
EMBEDDING IN YOUR PRIVACY PROGRAM

Privacy Compliance Lifecycle

1. Privacy Governance
   - Identify
   - Assess
   - Execute
   - Monitor

2. Scope & Requirements Management
   - Policies, Procedures, Controls
   - Communication, Training & Awareness

3. Supporting Technologies
   - Privacy Notice & Disclosures
   - Cross-Border Transfers
   - Data Subject Rights
   - Records of Processing
   - Third Party Management
   - Privacy by Design & Default
   - Data Security
   - Breach Notification

3. Structured data
4. Unstructured data

Business & Technology Infrastructure

1. Legal Basis for Processing
2. Consent Management
3. Privacy Impact Assessments
4. Cross-Border Transfers
5. Data Subject Rights
6. Records of Processing
7. Third Party Management
8. Privacy by Design & Default
9. Data Security
10. Breach Notification

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
UNDERSTANDING YOUR ENVIRONMENT

1. Governance & Change Management
   • Key Roles & Responsibilities
   • Standards & Templates

2. Privacy Impact Assessment Process

3. Privacy Engineering Framework

DevOps
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.

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.
EMBEDDING PRIVACY IN YOUR ORGANIZATION

1. Governance & Change Management

2. 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

3. Privacy Engineering Framework
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
5. Identify Privacy Controls
6. Identify the need for DPIA
7. DPO Review & Approval
8. Integrate into SDLC

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

© 2020 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
PRIVACY BY DESIGN FOR DEVELOPMENT

1. Governance & Change Management

2. Privacy Impact Assessment Process

3. Privacy Engineering Framework

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

**Privacy Requirements Definition**
- 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

**Privacy Strategy Selection & Design**
- 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.

**Privacy Controls Validation**
- 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

**Initiation of Data Processing**
- 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

**Secure Data Disposal**
- 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

**SDLC Phases**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiation</strong></td>
<td>Defining the scope and conducting initial Privacy Impact Analysis (PIA)</td>
</tr>
</tbody>
</table>
| **Design & Development** | 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. |
| **Implementation & Assessment** | It includes system installation and evaluation in organization’s environment.
  - Integrate information system
  - Plan system certification and security controls testing activities
  - Conduct system accreditation |
| **Operation & Maintenance** | It includes operating systems, tested enhancements, and hardware/software replacement.
  - Conduct operational readiness review
  - Manage system configuration
  - Monitor information system’s controls
  - Perform reauthorization |
| **Disposal**         | It provides system disposal, information archival, and contracts closeout.    |

© 2020 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
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.

DATA ORIENTED STRATEGIES
- Minimize
- Separate
- Abstract
- Hide
- Enforce & Demonstrate

PROCESS ORIENTED STRATEGIES
- Inform & Control
- Supervise

INFORM & CONTROL
- Log
- Audit
- Report

ENFORCE & DEMONSTRATE
- Create
- Maintain
- Uphold

ABSTRACT
- Summarize
- Group
- Obfuscate
- Dissociate

HIDE
- Strip
- Restrict
- Mix

SEPARATE
- Destroy
- Isolate
- Exclude
- Select

DISTRIBUTE
- Create
- Maintain
- Uphold

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.
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

1. Technically Difficult
   - 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.

2. Time Consuming
   - 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.

3. Legally Complex
   - 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

1998 - 2000

International Safe Harbor Privacy Principles
Principles developed in order to prevent private organizations within EU or US, which may store personal information, from accidently disclosing or losing this data

2013

Surveillance Exposed
Former U.S. Central Intelligence Agency contractor (Snowden), publicly exposed numerous global surveillance programs administered by the U.S. National Security Agency ("NSA")

2015

Facebook
Schrems successfully argued that Facebook’s privacy practices did not provide “adequate protection” of fundamental privacy rights as required under Article 25 of the Data Protection Directive.

Safe Harbor
European Court of Justice declared the International Safe Harbor Privacy Principles invalid - that later became known as “Schrems I”

2016

Privacy Shield
EU-US Privacy Shield framework for regulating transatlantic exchanges of personal information was adopted

2020

Privacy Shield
Invalidated
European Court of Justice invalidated Privacy Shield on which more than 5,000 companies relied on – referred to as the ”Schrems II” case

Maximilian Schrems is an Austrian activist who became known for his complaints against Facebook for violation of EU privacy law and alleged transfer of personal data to the U.S. National Security Agency (NSA).
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

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.
HOW CAN YOU PREPARE?

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

Understand the data privacy impact to the organization

Privacy requires support from all business areas

Understand all areas where data is captured and shared

Identify impacts from Privacy Shield and potential solutions

Versatile, agile and start now
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.
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 (ROP):** 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:**
- **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).

**Business Outcomes:**
- **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**

**Privacy Solutions & Privacy as a Service**

Our Software Partners:

- OneTrust
- Spirion
- Prevalent
- Informatica

© 2020 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
### TECHNOLOGY CONSULTING - SOLUTION OVERVIEW

<table>
<thead>
<tr>
<th>Technology Strategy and Operations</th>
<th>Enterprise Application Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Technology Strategy and Architecture&lt;br&gt;• Technology Governance and Risk Management&lt;br&gt;• Transformation Program Execution&lt;br&gt;• Technology Operations and Delivery</td>
<td>• Solution Design and Selection&lt;br&gt;• Implementation Support&lt;br&gt;• Application Security and Controls&lt;br&gt;• Point Solution Implementation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security and Privacy</th>
<th>Software Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security and Privacy Program and Strategy&lt;br&gt;• Cyber Security Operations and Implementation&lt;br&gt;• Digital Identity and Access Management&lt;br&gt;• Technical Security and Data Security and Privacy&lt;br&gt;• Incident Response, Forensics and Recovery</td>
<td>• Custom Business Applications&lt;br&gt;• Cloud, Portals and Collaboration&lt;br&gt;• Website Design and Solutions&lt;br&gt;• Intelligent Automation Enablement&lt;br&gt;• On-Demand Services and GRC Solution Implementation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud Solutions</th>
<th>Enterprise Data and Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cloud Strategy and Architecture&lt;br&gt;• Cloud Applications&lt;br&gt;• Cloud Modernization&lt;br&gt;• Cloud Security</td>
<td>• Enterprise Data Governance&lt;br&gt;• Enterprise Information Management&lt;br&gt;• Reporting and Visualization&lt;br&gt;• Digital Transformation and Software Services&lt;br&gt;• Business Strategy and Advanced Analytics</td>
</tr>
</tbody>
</table>
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