Information Privacy Decoded

The Five Elements of Proactive Privacy Stewardship

16 December 2021

Scott Foote, Phenomenati Consulting

Introductions

- **I am…**
  - **a Privacy professional and advocate**
    - a Data Protection Officer (DPO), CIPM (IAPP), CDPSE (ISACA)
  - **a Security professional**
    - a Chief Information Security Officer (CISO), CISSP, CCSA, CCSP, CISM, etc.
  - **an Auditor**
    - CISA (ISACA), ISO 27001 Auditor, etc.

- **I am not…**
  - **A lawyer**
  - Always consult a *qualified* Privacy Attorney or Legal Practice in putting together your Privacy Program.

Five Elements of Proactive Privacy Stewardship

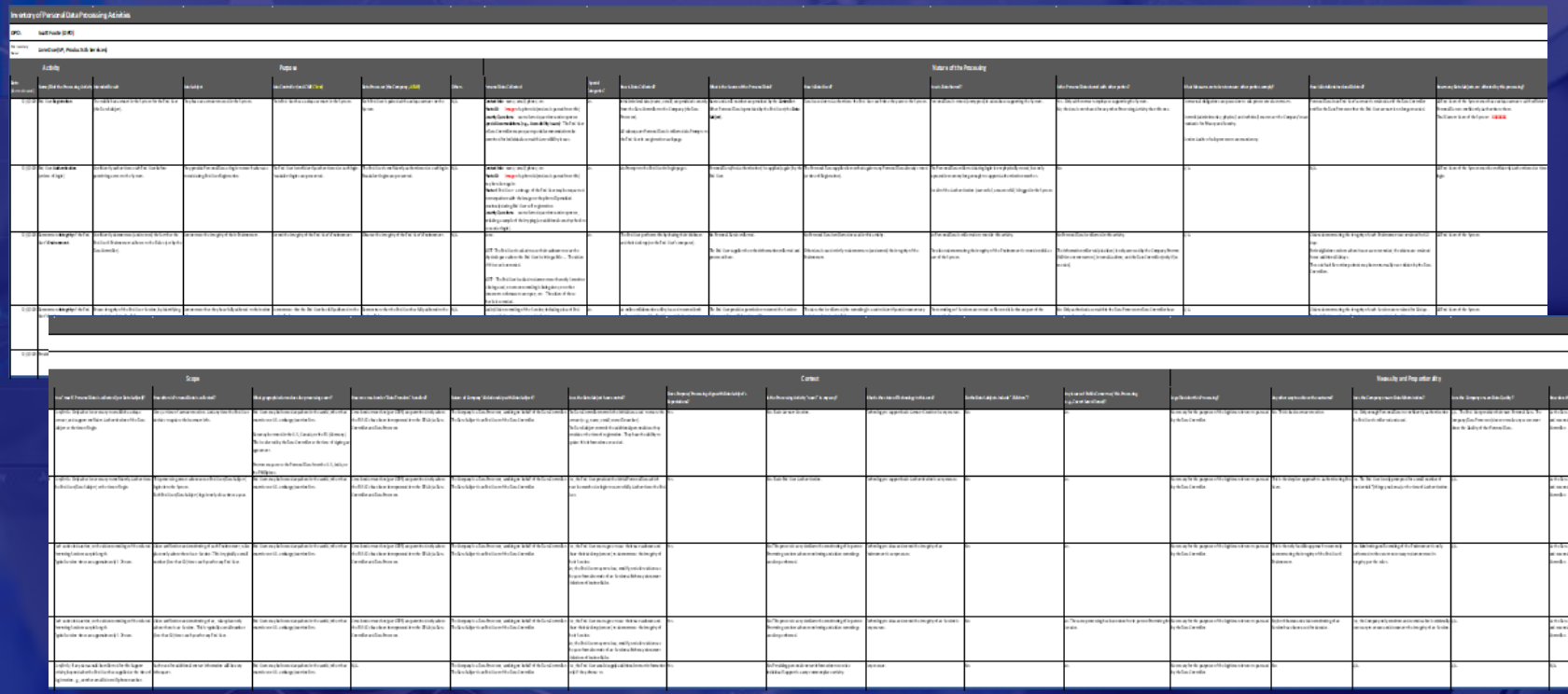
- **Reviewing the Foundations of a Privacy Program**
  - e.g., Who, What, Why, How, Where
- **Conducting Privacy "Risk Assessments"**
  - e.g., PIA, DPIA
- **Establishing Security & Privacy Controls**
  - e.g., Preventative, Detective, Corrective, Administrative, Physical, Technical
- **Building "Trust Through Transparency"**
  - e.g., Certification against Security & Privacy Standards – ISO/IEC 27001, 27017, 27018, 27701
  - e.g., Certification against Industry Regulations – PCI DSS, HITRUST
- **Engaging with the Subjects (people) of the Privacy Information**
  - e.g., Notice/Policy, Consent/Opt-In/Opt-Out,
  - e.g., Data Subject Requests, Notification of Breaches

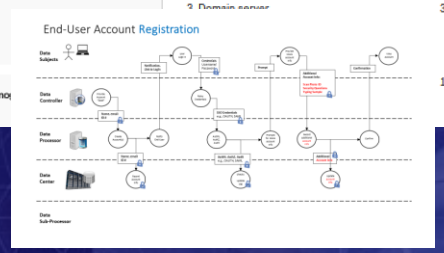
Foundations of a Privacy Program

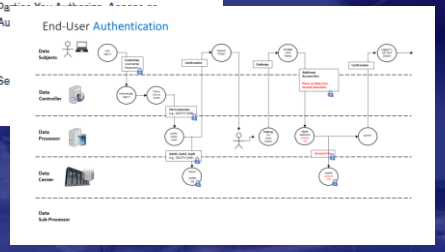
- **Scope**: Aspects of your Organization that are "In Scope" for Privacy
  - Marketing – target market demographics
  - Sales – contact information about prospects and clients
  - Employees – full-time and part-time staff, benefits info includes $ and Health privacy data
  - Vendors – contact information about vendors and service providers
  - End-Users of the Company's services
- **What**: Data Elements Considered in scope by Privacy Laws and Regulations
  - Non-Special Category Data
  - Special Category Data
  - Data Minimization: Are you collecting only the minimum PI/PII data necessary to achieve your organization's lawful purpose?
  - Consult a competent Privacy Attorney or Law Practice
- **Why**: Have you documented your lawful purpose for collecting/processing PI/PII?
  - Is Consent necessary? Given freely? Easily removed?
  - Is the PI/PII necessary "for the performance of a contract" to which the data subject is party?
  - Is the PI/PII necessary "for compliance with a legal obligation"?
  - Is the PI/PII necessary "to protect the vital interests of the data subject"?
  - Is the PI/PII necessary "to perform a task carried out in the public interest", or via official authority?
  - Is the PI/PII necessary "for the purposes of legitimate interests"?
- **How**: Is PI/PII Processed by (or on behalf of) your organization?
  - How is PI/PII collected? Directly, Indirectly, etc.
  - How is PI/PII processed?
  - How is PI/PII stored?
  - How LONG is PI/PII stored? (minimize Data Retention)
  - Have you documented all of the Data Flows of PI/PII through your organization?
- **Who**: Processes the PI/PII you collect?
  - Internal parties with access to PI/PII
  - External parties with access to PI/PII
- **Where**: Are the Locations of
  - Data Collection
  - Data Storage
  - Data Processing
  - Data Accesses

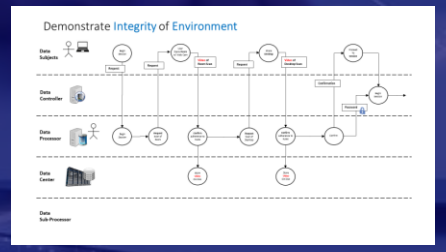
Foundations of a Privacy Program – Inventories & Diagrams

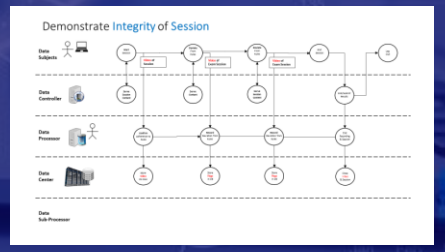
What this Online Privacy Policy Covers	Examples of Personal Data We Collect	Categories of Third Parties With Whom We Share this Personal Data:
Account or Contact Data	1. First and last name 2. Email 3. Postal address 4. Phone number 5. Unique identifiers such as passwords	1. Bank partners, other financial institutions and financial services companies 2. Service Providers 3. Postal address 4. Parties You Authorize, Access or Authenticate
Customer records identified by state law	1. First and last name 2. Social Security number 3. Address 4. Phone number 5. Tokenized bank account information, debit card information, other financial information	1. Bank partners, other financial institutions and financial services companies 2. Service Providers 3. Postal address 4. Parties You Authorize, Access or Authenticate
Customer records identified by state law	1. bank account number 2. debit card information 3. Payment card type 4. Billing address, phone number, and email 5. Account balance, transactional histories and other financial information	1. Service Providers (specifically Plaid, as described below) 2. Bank Partners 3. Parties You Authorize, Access or Authenticate
Commercial Data	1. Transaction history associated with your bank accounts and cards 2. Purchase history 3. Records of personal property, products or services obtained, or considered 4. Consumer profiles 5. Purchasing or consuming tendencies	1. Service Providers (specifically Plaid, as described below) 2. Parties You Authorize, Access or Authenticate
Device/IP Data	1. IP address 2. Device ID 3. Domain server 4. Type of device/operating system/browser used to access the Services	1. Know-your-customer (KYC) service providers 2. Parties You Authorize, Access or Authenticate
Web Analytics	1. IP address 2. Device ID	1. Service Providers 2. Business Partners
Consumer Demo		1. Se

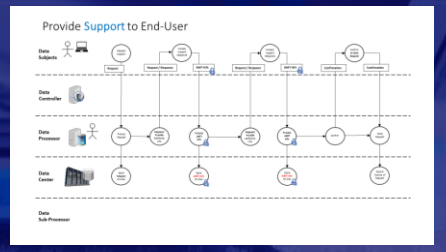












Conducting Privacy "Risk Assessments"

- **Privacy** Impact Assessment (**PIA**)
  - For new business systems, or changes to existing systems…
    1) Will any Personal Information (PI) or Personally Identifiable Information (PII) be impacted?
    2) If so, identify the potential "Risks to the Rights and Freedoms" of the relevant Data Subjects.
    3) Perform a Privacy Threshold Analysis (PTA)

- **Data Protection** Impact Assessment (**DPIA**)
  - Has each Risk identified (e.g., in PIAs) along the Data Flows, been assessed either Qualitatively, Quantitatively, or both?
  - These Risk Assessments should consider existing…
    a) Inherent Risk,
    b) Existing Controls,
    c) Residual Risk, and
    d) whether that Residual Risk should be Accepted, Rejected, Further Mitigated, or Transferred (not easily done with Privacy issues).

Establishing Security & Privacy Controls

- **For each Risk identified in your Assessments (PIA, DPIA)…**
  - Have you identified a set of **relevant Security & Privacy Controls** to mitigate that Risk?
  - Administrative, Physical, Technical Controls
  - Preventative, Detective, *Corrective* Controls

- **For any/each Cross-Border Transfer of PI/PII**
  - Has an appropriate Control been established to ensure protection of the Privacy in the new geographic region?
  - e.g., GDPR requires one of…
    - adequacy decisions,
    - Standard Contractual Clauses (SCC),
    - Binding Corporate Rules (BCR), etc.

- **Are you anonymizing or pseudonymizing PI/PII in any way?**

Cyber Security Controls Landscape

Stage of Compromise

Control Type	Preventative	Detective	Corrective
Technical	e.g., Authentication e.g., Authorization e.g., FWs, Gateways, Proxies e.g., Data Loss Prevention	e.g., Audit Trails (logs) e.g., Detection Analytics e.g., Honeypots/nets e.g., Canaries (“DRM”)	e.g., Traffic Redirect e.g., Account Lock e.g., Software/System Quarantine e.g., System Restore
Administrative	e.g., Policies & Procedures e.g., NDAs, Security Training e.g., Patch Management e.g., Principle of Least Privs	e.g., Auditing / Threat Hunting e.g., Separation of Duties e.g., Job Rotation e.g., Risk ID & Assessment	e.g., Disaster Recovery Plan e.g., Business Continuity Plan e.g., Cyber Insurance
Physical	e.g., Guards, Gates, Badges e.g., Locks, Secure Areas e.g., Encryption	e.g., Audio/Video Surveillance e.g., RFID, GPS e.g., Heat Sensors	e.g., Fire Suppression e.g., Redundant Systems/Site e.g., Restore from Backup

Engaging with the Subjects of the Privacy Information

- **Notice: Transparency of processing with the Data Subjects affected?**
  - Are your Privacy Policies easily understood, and immediately accessible at the time/place of data collection?

- **Consent: Is Consent needed? How/When is it obtained? Can it easily be revoked?**
  - Opt-In e.g., GDPR, and very likely all future legislation
  - Opt-Out e.g., default in the U.S., and growing increasingly unpopular

- **Establish a "Data Subject Requests (DSR) Program" to formally handle requests**
  - Ability for Data Subjects to restrict the processing of their PI/PII?
  - Ability for Data Subjects to object to automated decision-making or profiling, based upon the PI/PII your organization collects on them?
  - Access to the PI/PII for the Data Subjects affected?
  - Ability to correct (rectify errors) PI/PII for the Data Subjects affected?
  - Ability for the Data Subject to export their PI/PII for transfer to a similar system (where appropriate)?
  - Right to be forgotten… ability to request PI/PII be erased… balanced with the legal or regulatory obligations for Data Retention.

- **Breach Notification Obligation(s)**
  - Has your organization prepared appropriate communications (content and services) for use in the event of a privacy data breach?

Trust Through Transparency

- 3rd Party Compliance Audits / Certifications

- Certification against Security & Privacy Standards
  - ISO/IEC 27001 – requirements for an Information Security Management System (ISMS)
  - ISO/IEC 27017 – security of cloud services
  - ISO/IEC 27018 – data privacy in cloud services
  - ISO/IEC 27701 – extends 27001 for Privacy Information Management

- Certification against Industry Regulations, Standards, and Frameworks
  - PCI DSS – Payment Card Industry Data Security Standard
  - HIPAA, HITRUST CSF

Questions?