



# IAPP Privacy Certification<sup>1</sup>

Certified Information Privacy Professional (CIPP)

## Data Sharing & Transfer

**Bryan Tretick**

Principal

 **ERNST & YOUNG**

# agenda

2

- **company inventory**
- **privacy policy**
- **common terminology**
- **user preference strategy**
- **access & redress**
- **transfer of information**

# agenda

- **international data**
- **oversight & governance**



# Data Sharing and Transfer

4

# company inventory

- **Purpose of Inventory**
  - **Proactive & Reactive reasons**
- **Organization Chart**
- **Physical location of data storage**
  - **Domestic**
  - **Outside US**
  - **Accountability**

## **company inventory**

- **For each type of PII data**
  - **Location of data**
  - **Data ownership**
  - **Level of sensitivity and protection (e.g. encryption)**
  - **Process flow use and maintenance**
  - **Trans-border**
  - **Dependency on other systems**

## company inventory

- **Purpose & Users of PII** 7
  - How is data shared with other companies
  - Reasons specified
  - Who has access & How is it controlled



# Data Sharing and Transfer

8

# privacy policy



# OECD guidelines

- **A basic framework since 1980**
  - **Collection limitation principle**
  - **Data quality principle**
  - **Purpose specification principle**
  - **Use limitation principle**
  - **Security safeguards principle**
  - **Openness principle**
  - **Individual participation principle**
  - **Accountability principle**

# privacy policy

- **Single Policy or Multiple**
- **Approval of Policy & Revisions**
- **Training & Awareness**
- **Communication to Audience**
  - **Annual Notice**
  - **Post on location**
  - **Post online**
- **Version Control**

# privacy policy

- **Disclosure of information collected** 11
  - Name, address, cookies, financial information, etc.
- **Disclosure of info. use, sharing & choice**
  - Name, address & purchase history
  - Internal purposes, marketing efforts, analysis, service provider, sharing with third parties for their benefit.
  - Opt Out/Opt In

# privacy policy

- **Disclosure of Process**
  - Access & redress, change in policy, etc.



# Data Sharing and Transfer

13

**common  
terminology**



**common  
terminology**

- **Know common terminology and its applicability**
  - **PII, PHI, NPI, personal data, etc.**



# Data Sharing and Transfer

15

**user preference  
strategy**

## user preference strategy

- **Opt Out or Opt In**
- **Channels** - online, call center, VRU, brick and mortar, etc.
- **Applying preferences** - by account number, name, email, household, etc.
- **Confirmations**
- **Preference changes** - verbal, written, online form, etc.
- **Honoring preference** - specified time period, forever, etc.



## user preference strategy

- **No Opt**
  - **Viability and Risks**
  - **Legal/Regulatory Exceptions:**
    - **joint marketing between financial institutions, service provider, subpoena**
- **Acquiring preferences from third parties or affiliates & subsidiaries**
  - **Ensuring integrity**
  - **Honoring pre-existing preference elections**
  - **Compare with privacy strategy**



**user  
preference  
strategy**

- **Maintaining Customer Preference**
  - **Acquired preferences from 3<sup>rd</sup> parties, affiliates, subsidiaries**
  - **Managing preferences by product line or service variety**
  - **Making changes to preferences**
- **Honoring Customer Preferences**
  - **Joint Marketing Agreements**
  - **Affiliates or Subsidiaries**
  - **Product Line and Service Variety**
  - **Federal & State Laws**



# Data Sharing and Transfer

19

# access & redress

## **access & redress**

- **Process Disclosure**
- **Compliance with EU Directive or other applicable laws.**
- **Customer changes within one company or one division**



## Data Sharing and Transfer

21

# transfer of information

## transfer of information

22

- **Sharing with affiliates, subsidiaries or third parties**
- **Contract and Vendor Management**
  - (1) **Due diligence**
    - **Reputation**
    - **Financial condition**
    - **Information security controls**

## transfer of information

- **Information security controls (detail):**
  - **Access**
  - **Audits**
  - **Disposal of information**
  - **DR/BRCP**
  - **Firewalls**
  - **Insurance**
  - **Intrusion detection**
  - **Incident response**
  - **Physical security**
  - **Training & awareness**

**transfer of  
information**

- **Contract and Vendor Management (contd)**

24

- (2) **Confidentiality provision**
- (3) **Further use of shared information**
- (4) **Use of sub-contractors**
- (5) **Requirements to notify**
- (6) **Background checks**
- (7) **Requirements to disclose breach**



**transfer of  
information**

25

- **Approval Process & Justification to Share New Information**
  - **Consistent with Privacy Policy**
  - **Review new applicable laws & enforcement actions**
  - **Business Need**



# Data Sharing and Transfer

26

# international data

- **Exceptions to Global Policy**
  - **Process**
- **Transfer of info. overseas (outsourcing/vendor/affiliate)**
  - **Safe harbor/standard model contract/Article 29 Working Party**
  - **Customer Consent**
  - **Notification to foreign govt. authorities**

**international  
data**

- **International Terminology**

- **Data subject, data controller, data processor, personal data**

- **Conducting Business Overseas**
  - **Employee vs. Customer Data**
  - **Phone lists, vendor info, benefits**
- **Marketing Overseas**
  - **Opt In/Opt Out**
  - **Customer Consent**
  - **Phone, email, direct mail, instant messaging, text messaging**
- **Policy for International Law**
  - **Country-specific or Global**



## Data Sharing and Transfer

30

# oversight & governance

**oversight  
&  
governance**

- **Monitoring Disclosure and Preference**
- **Management Activity**  
(compliance w/policy)
- **Self Assessments**
- **Third Party Audits**
- **Certifications**
- **Training & Awareness**
- **Physical & Information Security**
- **Security + Privacy**



**IAPP Certification** Promoting Privacy