ZASIO

Identifying and Breaking Down Privacy Requirements for Your Program

Brandon Tuley
CIPP-E
Analyst, Zasio

Items to Note

- If you would like to participate, use the side panel controls to ask a question. Zasio will respond after the webinar via email.
- We will email attendees a copy of this recording along with responses to additional questions or comments. If you don't want to receive any follow up in regard to this session, please send me a note in the chat box and I will consider that your "opt out".
- Thank you for the questions you all submitted in advance!

The information provided in this presentation is not legal or other professional advice and should not be construed as an advertisement for legal or professional services; instead, all information presented is for general informational purposes only. Opinions are from the presenters, and do not represent the views of Zasio.

Esteemed Guest & Discussion Leaders

Brandon Tuley, JD, CIPP/E,
Analyst / Licensed Attorney

Jennifer Chadband, JD, CRM, CIPP/E, IGP, ECMp
Sr. Analyst / Licensed Attorney

Rick Surber, JD, IGP, CRM
Sr. Analyst / Licensed Attorney

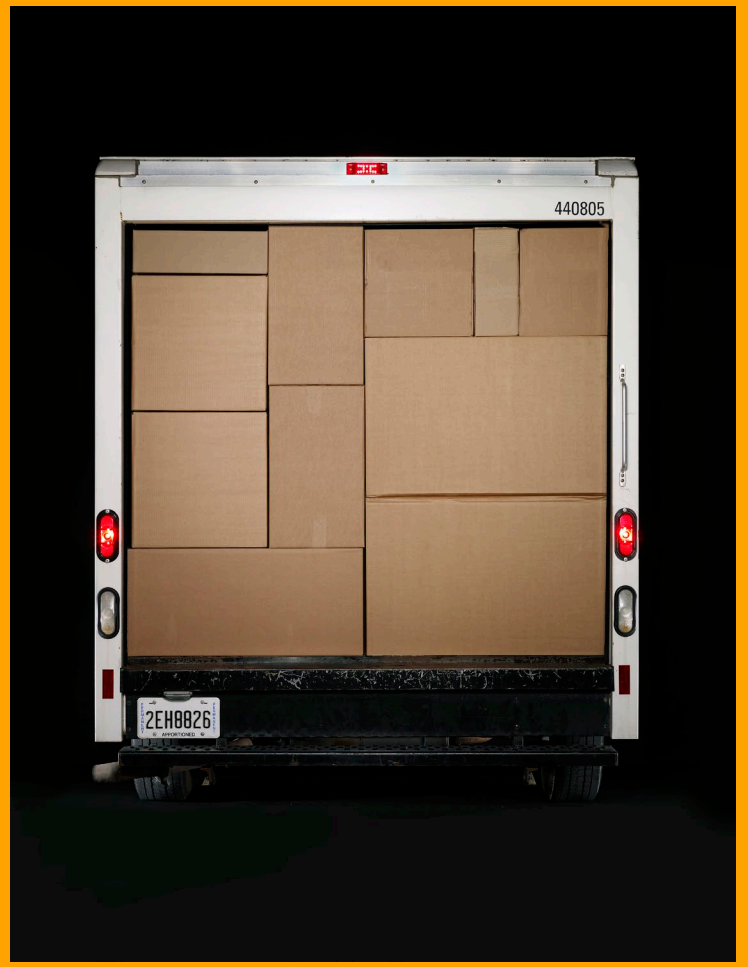
ZASIO

Discussion Roadmap

- Common and Integral Categories
  - Regulated parties
  - Personal information
  - Breach notifications
  - Data subject requests
  - Cross-border transfers

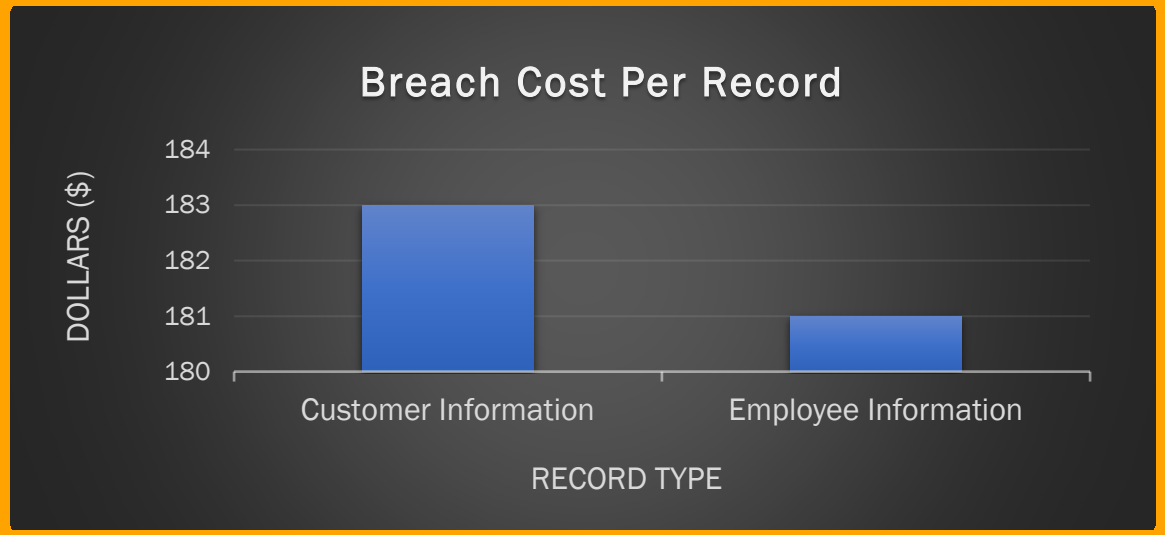
Identifying and Breaking Down Privacy Requirements

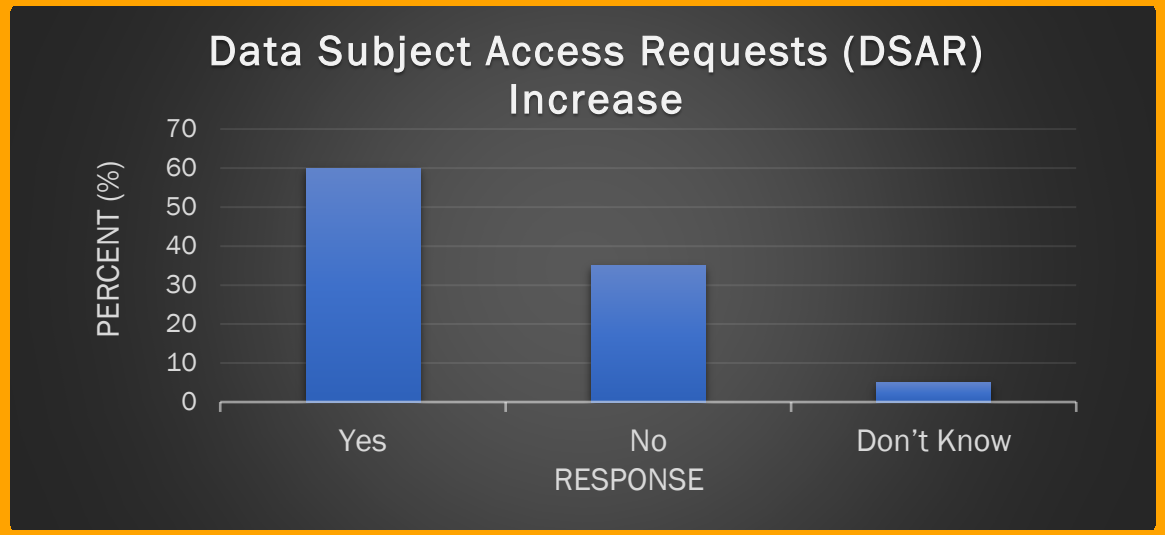
- Strategies to Simplify Privacy Requirements
  - Identify commonly regulated concepts
  - Sort provisions into categories
  - Compare and contrast requirements between jurisdictions



Importance of Today's Discussion

- Knowledge of requirements
- Financial implications
- Increased volume of compliance activities





Where to Begin – Analyzing Applicability

- Where do we operate and provide services?
- Who is regulated by the requirements?
- What information is governed?

Regulated Parties

- United States common concepts
  - Exemptions
    - Entity level
      - Numerical thresholds
      - Institutions subject to the GLBA, HIPAA, etc.
    - Topic level
      - Employee and applicant information
      - Information subject to the GLBA, HIPAA, FCRA, etc.
- Common concepts outside the United States
  - Absence of numerical thresholds
  - Limited number of situations entirely exempt

Regulated Parties – Comprehensive Privacy Laws

Jurisdictions	Data Controller Definition	Thresholds		
		Revenue	Processing	Sales
California 	Any entity that collects consumers' personal information, or on the behalf of which such information is collected, and alone or jointly with others determine the purposes and means of processing consumers' personal information	Gross annual revenue over **$25 million**	Buy, sell, or share the personal information of **100,000 or more** residents, households, or devices	Derive **50%** or more of their annual revenue from selling residents' personal information
Colorado 	Any entity that alone or jointly with others, determine the purposes for and means of processing personal data		Process the personal data of **more than 100,000** residents in any calendar year	Derive revenue or receive discounts on goods or services in exchange for the sale of personal data of **25,000 or more** residents
European Union 	Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data			

Regulated Parties – Comprehensive Privacy Laws

Jurisdiction	Nonprofits	Institutions Subject to GLBA	Information Subject to GLBA	Institutions Subject to HIPAA	Information Subject to HIPAA	Information Subject to FCRA	Information Collected for Clinical Trial	Employee or Applicant Information
California 	Exempt		Exempt		Exempt (personal health data)	Exempt	Exempt	
Colorado 		Exempt	Exempt		Exempt	Exempt	Exempt	Exempt

US Federal Law	Regulated Entities	Purpose
Gramm-Leach-Bliley Act (GLBA)	Financial institutions	Mandates privacy notices and place limitations on the sharing of nonpublic personal information
Health Insurance Portability and Accountability Act (HIPAA)	Health plans and medical providers	Protects individuals' medical records and other individually identifiable health information
Fair Credit Reporting Act (FCRA)	Collectors and reporters of consumer credit information	Promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies

Regulated Parties – Comprehensive Privacy Laws

Jurisdictions	General Exemptions
European Union 	- During an activity which falls outside the scope of Union law; - By a natural person conducting a purely personal or household activity; - By Member States carrying out activities that are within the common security and defense policy; and - By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security - Article 23 restrictions - Chapter 9

Regulated Parties – Breach Notifications

Jurisdictions	Regulated Parties
California 	"Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.
Colorado 	"Person" means an individual, corporation, business trust, estate, trust, partnership, unincorporated association, or two or more thereof having a joint or common interest, or any other legal or commercial entity.
European Union 	"Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Personal Information Definitions

- United States common concepts
  - State consumer privacy laws → Broad definition
  - Breach notification laws → Data element combinations
- Common concepts outside the United States
  - Defined consistently and in a broad manner

Personal Information Definitions

Jurisdictions	Breach Notifications	Comprehensive Privacy
California 	"Personal information" means either of the following: - An individual's first name or first initial and last name **in combination with any one or more of the following data elements**, when either the name or the data elements are not encrypted:.....; or	"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
Colorado 	"Personal information" means a Colorado resident's: - First name or first initial and last name in combination **with any one or more of the following data elements** that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:.....;	"Personal data" means information that is linked or reasonably linkable to an identified or identifiable individual
European Union 	"Personal data" means any information relating to an identified or identifiable natural person ('data subject')	"Personal data" means any information relating to an identified or identifiable natural person ('data subject').

Analyzing Applicability – Program Considerations

- Operational footprint
- Regulated party definitions
  - Exemptions
    - United States
      - Entity level
      - Topic level
    - Outside the United States
      - Rarely apply
- Personal information definitions
  - United States
    - Breach → Data elements required
    - Comprehensive → Broadly defined
  - Outside the United States
    - Defined in same manner

Commonly Regulated Concepts

- Breach notifications
- Data subject requests
- Cross border transfers

Commonly Regulated Concepts - Breach Notifications

- Who to notify
  - Data subjects
  - Governmental entities
  - Consumer reporting agencies
- Conditions to notify
  - Thresholds
- Timeline to notify
  - Without unreasonable delay
  - In the most expedient time possible
  - Not later than

Processes for Breach Notifications

Jurisdictions	Who to Notify	Conditions to Notify	Timelines to Notify
California 	Data subject	Following discovery or notification of the breach in the security of the data	In the most expedient time possible and without unreasonable delay
	Attorney General	Required to issue a security breach notification to **more than 500 California residents**	
Colorado 	Data subject	Determine that the misuse of information about a Colorado resident has occurred or is reasonably likely to occur	In the most expedient time possible and without unreasonable delay, **but not later than 30 days** after determining that a security breach occurred
	Attorney General	Reasonably believe a security breach is to have affected **500 Colorado residents or more**	In the most expedient time possible and without unreasonable delay, **but not later than 30 days** after determining that a security breach occurred
	Credit reporting agencies	Required to notify **more than 1,000 Colorado residents** of a security breach	In the most expedient time possible and without unreasonable delay
European Union 	Data subject	Breach is likely to result in a **high risk** to the rights and freedoms of natural persons	Without undue delay
	Supervisory authority	Breach is likely to result in a **risk** to the rights and freedoms of natural persons	Without undue delay and **where feasible within 72 hours** of becoming aware of the breach

Program Considerations – Breach Notifications

- Who to notify
- Conditions to notify
  - Numerical conditions
  - Severity of harm
- Timelines to notify
  - As soon as possible, without unreasonable delay, without undue delay
  - Maximum time allowed to notify

Commonly Regulated Concepts – Data Subject Requests

- Request and response types
- Timelines to respond
- Extensions
  - Notice
- Record-keeping requirements

Processes for Data Subject Requests

Jurisdictions	Request Types	Timelines to Respond	Extensions	Record-Keeping
California 	Know, Correct, Delete	Confirm receipt of the request within **10 business days** after receiving the request Respond with action taken within **45 calendar days** after receipt of the request	**45 more days** (90 days total) so long as the data subject is notified	Requests and responses must be kept for **at least 24 months**
Colorado 	Access, Correct, Delete, Opt Out, Portability	Respond with action taken within **45 days** after receipt of the request	**45 more days** (90 days total) so long as the data subject is notified	Consumer requests and responses must be kept for **at least 24 months**
European Union 	Access, Rectify, Erasure, Restrict, Portability, Object, Not be Subject to Automated Decision Making	Respond with action taken within **1 month** of receipt of the request	**2 more months** so long as the data subject is notified	
Hong Kong 	Access, Correct	Respond with action taken within **40 days** after receiving the request		Refusals to comply with the request to access or correct must be kept for **4 years** after the day of information entry

Program Considerations – Data Subject Requests

- Request types
- Response deadlines
  - Calculating response times
- Extensions
  - Notice
- Record-keeping
  - Global retention period

Commonly Regulated Concepts – Cross Border Transfers

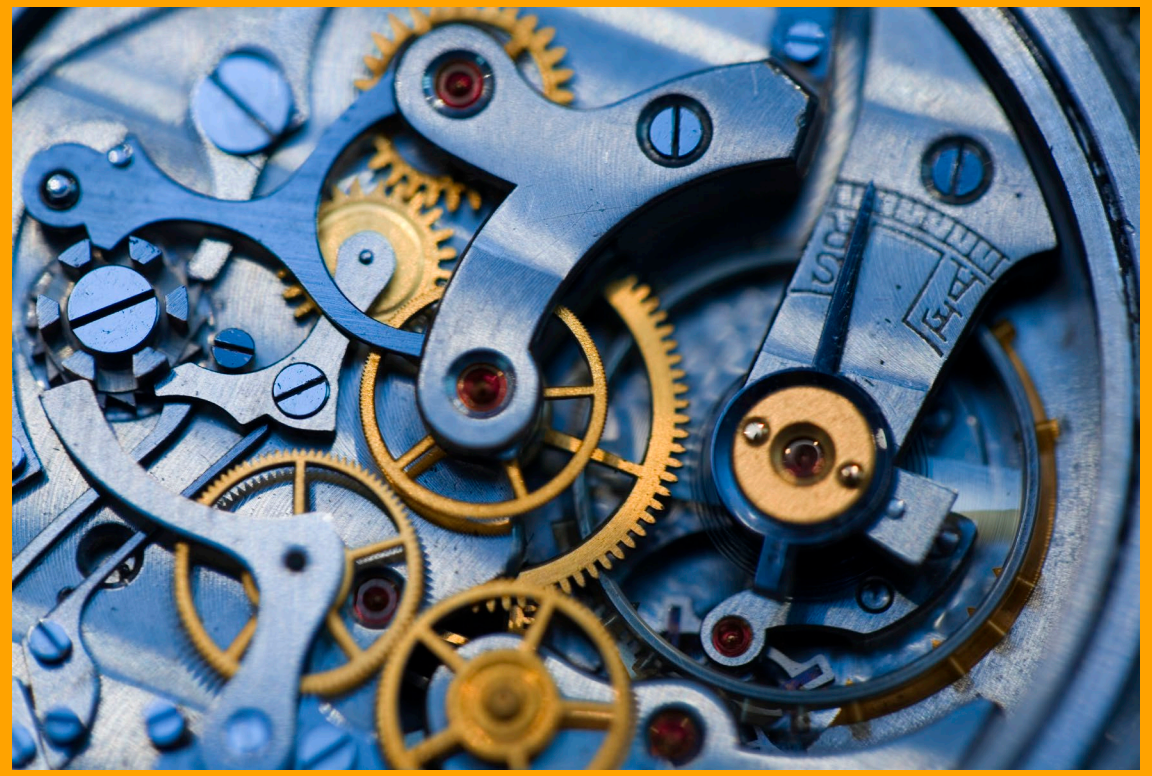
- Localization requirements
  - Uncommon
- Transfer impact assessments
- Notice
  - Content

Processes for Cross Border Transfers

Jurisdictions	Localization Requirements	Impact Assessments	Notice of Transfer
European Union 		**Recommended** by the European Data Protection Board to transfer data outside the EEA	- Intent to transfer personal data to a third country; - Existence or absence of adequacy decision; and - Reference to appropriate safeguards if transfer is made in the absence of adequacy decision
Québec 		Must conduct a privacy impact assessment before communicating personal information outside Québec	Possibility that the information could be communicated outside Québec
Vietnam 	Domestic enterprises **must keep the following in Vietnam:** - Personal information of service users in Vietnam; - Data created by service users in Vietnam of service account name, service usage time, credit card information, email address, registered network (IP) address most recent login, logout, and registered phone number attached to the account; and - Data about service users' relationships in Vietnam of friends and groups with which users connect or interact	Impact assessment of outward transfer of personal data must be completed to transfer data abroad	Consent of data subject

Program Considerations – Cross Border Transfers

- Localization requirements
  - Uncommon
  - Review applicability
- Transfer impact assessments
- Notice
  - Content



Program Considerations – Bringing it Together

- Determine applicability
- Identify commonly regulated topics and subtopics
- Valuable resources
  - Definition section
  - Government websites
  - Guidelines
- RRS and program component integration

Contact Info:

Brandon R. Tuley
Zasio Enterprises, Inc.

brandon.tuley@zasio.com

www.linkedin.com/in/brandon-tuley

Join Us!

- Thursday, Feb. 15, 2024
- See newsletter, emails for registration details