Privacy Around the World in 60 Minutes

Regional Compliance & Ethics Conference | Minneapolis
March 1, 2019

This Session Uses Polling

To Participate in polling

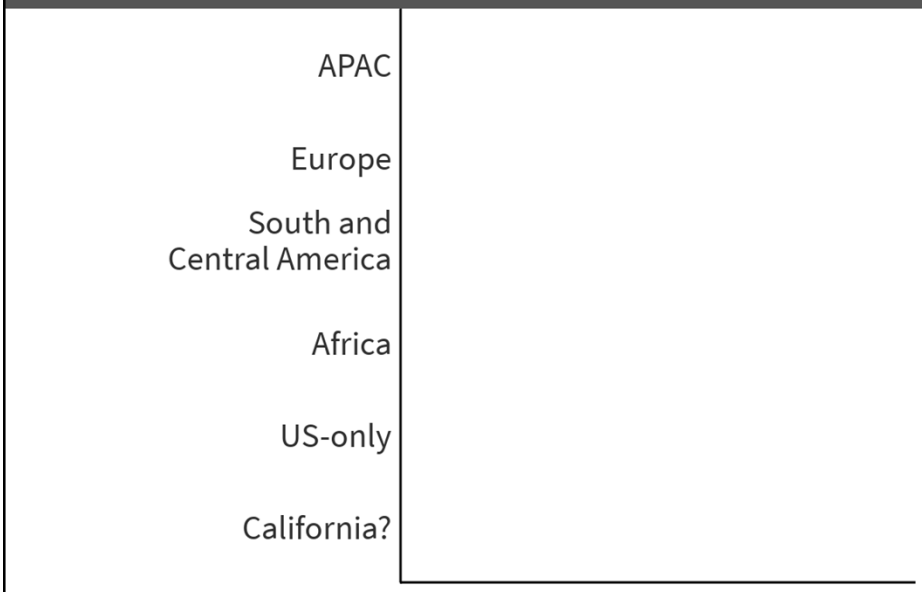
Download “SCCE Mobile” in your app store. Then under the agenda find this session , scroll to the bottom and click “Poll Questions” or go to PollEv.com/SCCE

PRESENTED BY OPTUM PRIVACY TEAM MEMBERS:

Donna Kasbohm
Senior Director, Senior Associate Counsel, Optum Privacy

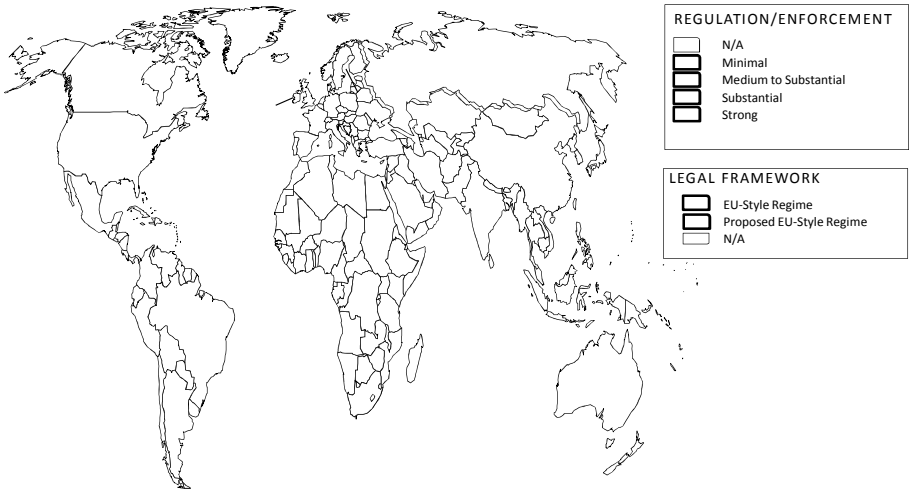
Sarah Boswell-Healey
Director, Global Privacy

Where are you concerned with privacy compliance?



Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app

Current State – Global Privacy Laws



Current State – Global Privacy Laws

Data Protection Laws across the world are changing rapidly; GDPR is the new standard

- Japan, Hong Kong, Brazil, India, Philippines
- Data Protection Maturity across APAC and AMEA
- China?

Adequacy Considerations: Privacy Shield?

Cross-border Data Transfers: Model Clauses; BCR

Brexit?

Intent – Changes to Global Privacy Laws

Key Objectives:

Ensure a high level of protection for individuals

Modernize data privacy laws

Ensure more robust enforcement

"Data protection laws exist to ensure fair play for everyone in how their identity and personal data is used by big corporations, governments and all sorts of organisations and businesses. ***The GDPR is a game- changing overhaul of our current data protection laws. It will impact every type of company and organisation regardless of their size*** *and require many of them to take significant action well before May 25th , 2018.*

- Helen Dixon, Data Protection Commissioner, Ireland
http://gdprandyou.ie/wp-content/uploads/2017/05/DPC-Press-Release-365-to-GDPR.pdf

"What must be recognised is that GDPR is an evolution in data protection, not a total revolution. ***It demands more of organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals****. GDPR is building on foundations already in place for the last 20 years."*
- Steve Wood, Deputy Commissioner (Policy) UK ICO
https://iconewsblog.org.uk/2017/08/25/gdpr-is-an-evolution-in-data-protection-not-a-burdensome-revolution/

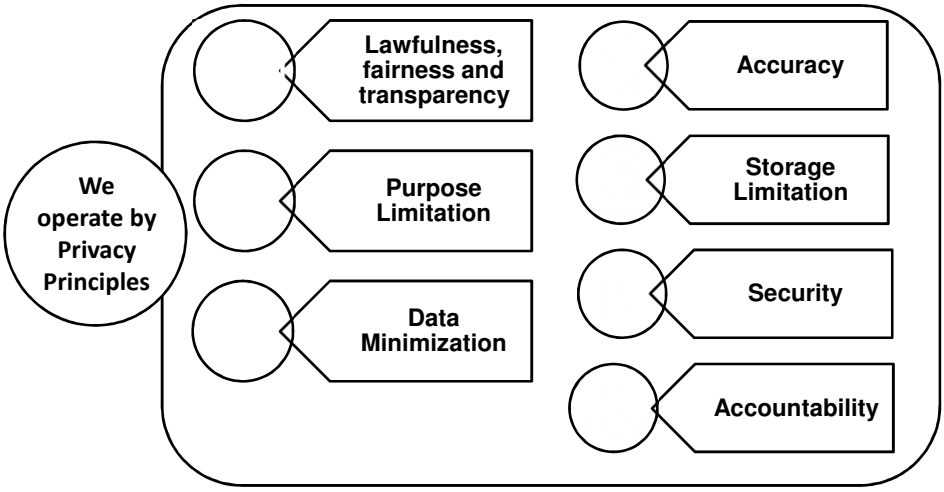
Louise has been working on a new service that sells weight loss nutrition bars. She also has access to a list of email addresses of patients that was collected in order to send doctor appointment reminders. She would like to use the email list she has for appointment reminders to market the new service. Is this an acceptable use of the email list?

Yes, we already have the email addresses, so we can use them for any legitimate business purpose.

No, we only collected the email addresses for the purpose of sending appointment reminders and so we can't use them for this other purpose.

Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app

What Is Required?: Privacy Principles



Privacy Principles

GDPR regulates "processing" of "personal data"

"processing" is defined very broadly – essentially covers doing anything with personal data (e.g., collecting, recording, organizing, structuring, storing, adapting, using, disseminating, combining, erasing, destroying)

"personal data" also is defined very broadly

information relating to an identified or identifiable natural person (a "data subject")

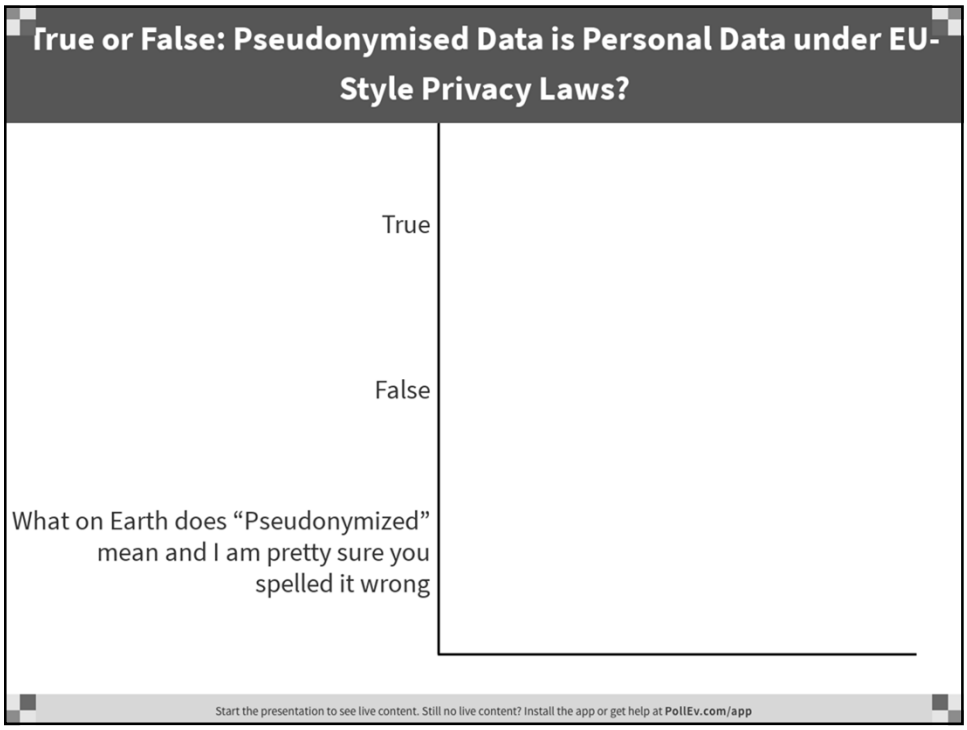
an identifiable natural person is one who can be identified, directly or indirectly, e.g., by reference to an identifier such as a name, an ID number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

GDPR applies to pseudonymous data (from which someone could be identifiable when combined with additional data held separately), but not truly anonymous data

Privacy Principles

Sensitive Personal Data (or "special categories of personal data") requires additional protection:

- Personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership;
- Genetic data
- Biometric data processed for the purpose of uniquely identifying a person; and
- Data concerning a person's health, sex life or sexual orientation



Privacy Principles

Anonymised Data, aka de-identified data, is data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place.

Anonymised/De-Identified data is typically outside scope of data privacy regulations; however, business limitations may still apply

Pseudonymisation is a process of assigning to individuals a unique identifier which does not reveal their "real world" identity. An example of a pseudonymisation technique is to replacement of a unique identifier with a randomly generated number

Personal Data

Pseudonymised Data

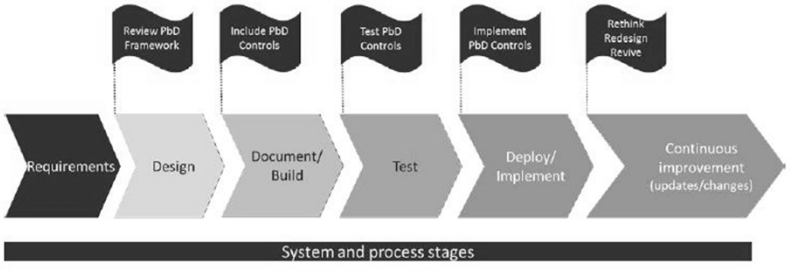
Non-Personal Data

Permanently Anonymised Data
Aggregate Data
Statistical Data

Privacy Principles

Privacy-by-Design (PbD) Privacy taken in account throughout the business and IT development lifecycle

By building PbD into systems and processes early in the development stage, we are able to meet compliance objectives, achieve cost savings, improve business performance, and increase customer confidence



Privacy Principles

A **Data Protection Impact Assessment (DPIA)** is a required assessment to review whether new processing of personal data or changes in the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. The DPIA also assists in identifying new or additional requirements.

The DPIA should be performed **before** initiating new processing or making changes in the processing of personal data

Privacy Principles

Individual Rights for EU Data Subjects include the *qualified* right to:

Access (Data Subject Access Request)

Be informed

Rectification

Erasure

Restrict Processing

Data Portability

Object

Rights relative to automated decision making and profiling

Privacy Principles

Incident Management and Breach Notification Requirements:

- 72-Hour Notification for Data Controllers, less time for Data Processors
- Risk to the Rights and Freedoms of natural persons? *High* Risk?
- Ensure procedures, tools, and resources are in place to effectively manage a privacy incident, including notifications to regulators, customers, or impacted individuals within required timelines
- Consider Cross Border Data Transfer implications of global incident management
- READ YOUR CUSTOMER AGREEMENTS
- Monitor regulatory changes in the Incident Management space (ex. Australia)

Is this a window on the future for US Incident investigation turn around times?

Australia Law Change as Example…..

Privacy Principles

What changed in the Law:

Privacy Amendment (The Notifiable Data Breaches Act 2017) Act 2017

As of February 22, 2018, Australian law changed its notification requirements to both the Commissioner and impacted individuals, from "Voluntary" to "Mandatory" for certain "eligible data breaches"

To whom does the Law apply?

The Law applies to: companies with existing obligations to comply under the Privacy Act must comply with the new mandatory reporting requirements

To what information does the Law apply?

Personal information is information about an identified individual, or an individual who is reasonably identifiable (alone or in combination)The mandatory data breach notifications include data breaches that relate to: Personal information; Credit Reporting Information; Credit eligibility information; or Tax file numbers

Privacy Principles

What is an "eligible data breach"?

An eligible data breach occurs when the following criteria are met:

• There is unauthorized access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorized access or disclosure is likely to occur)

• This is likely to result in serious harm to any of the individuals to whom the information relates

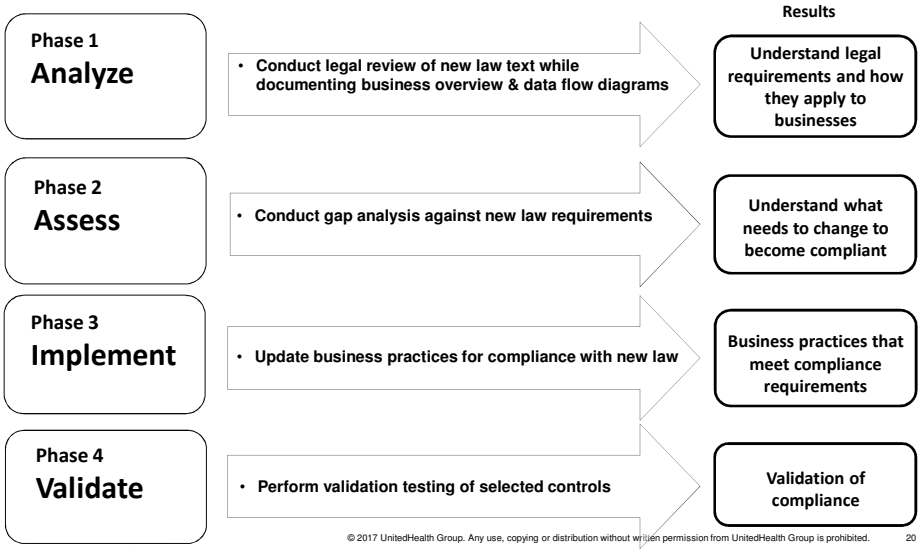
• The entity has been unable to prevent the likely risk of serious harm with remedial action

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations

Is serious harm likely?

- The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible)
- 'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm

Readiness Project Stages

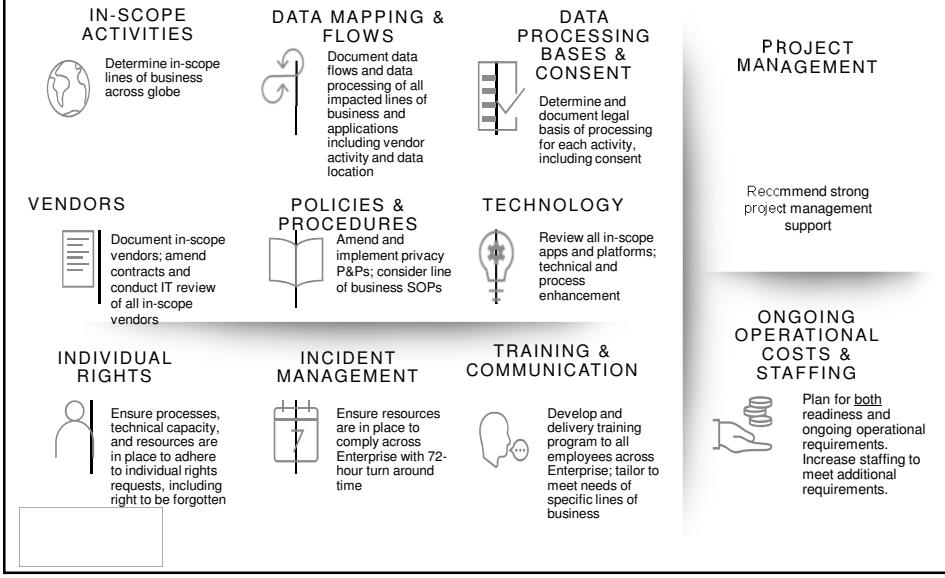


© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

What is Required to Implement EU (GDPR) Style Privacy Program: Areas of Attention

Focus areas	Description
Privacy governance	Data processing activities are legally permitted and documented, and that personnel are aware of appropriate data protection practices
Policy, privacy notices, and consent	Policies align with the new law requirements. Individuals are provided with notice, and the enterprise obtains valid consent (where necessary) prior to data processing
Individual rights	Procedures, tools, and resources are in place to effectively manage IR requests for access, correction, erasure, portability, and/or objection
Breach notification	Procedures, tools, and resources are in place to effectively manage a privacy incident, including notifications to regulators, customers, or impacted individuals within required timelines
Safeguards and controls	Privacy safeguards, including administrative and technical controls are implemented and maintained to protect personal data
Vendor management and data transfers	Third party due diligence is performed prior to contracting, contracts with third parties processing personal data have appropriate privacy provisions, including standard contractual clauses where cross-border data transfers occur
Communication and Training	Ensure new law training is performed before the law takes effect; engage in ample, iterative communication with leadership regarding impact of new law implementation; consider tailored trainings and in person training for highly impacted employee groups or teams; consider FAQs for customers and employees where appropriate

What is Required to Implement EU (GDPR) Style Privacy Program



Global Privacy Law Highlights

European Union (GDPR)

- The GDPR largely replaces existing country-specific data protection laws in the EU and directly applies to all Member States
- Broader territorial reach than current law, applying to:
  - processing of personal data that takes place "in the context of" activities of an establishment of a controller or processor in the EU – regardless of whether the processing takes place in the EU
  - processing by controller or processor outside the EU, but the processing relates to (1) offering goods or services to data subjects in the EU; or (2) monitoring the behavior of data subjects in the EU
- Legal basis for processing required, could be consent
- Expanded Individual Rights
- 72-hour TAT for individual and regulator notification
- DPO designation required
- Fines of up to 4% annual global revenue or 20 million euros, whichever is higher. Increased risk for class action lawsuits.

Brazil (LGPD)

- LGPD largely mirrors GDPR privacy provisions; goes live August 2020
- Extraterritorial reach applies to companies that process data in Brazil, obtain personal data from Brazil, or offer goods or services to individuals in Brazil
- Justification for processing data required; could be consent
- Expanded Individual Rights
- Breach notification required to individuals and regulator within a reasonable period of time
- DPO designation
- Fines of up to 2% gross Brazil revenue capped at approximately 13 mil USD; deletion of data or suspension of data processing activities possible.
- Current law consists of provisions across several laws, including the Brazilian Internet Law

Global Privacy Law Highlights

Chile

- Planning to replace current regulation with new law that will include EU-style data processing requirements (could pass early 2019?)
- *Current law* contains no obligation to report a breach
- *Current law* sanctions include fines up to 3.6k USD, possible criminal sanctions including jail time for a data breach
- DPO-like appointment required (Responsible Person)
- *Current law* requires public (but not private) data bases to be registered

China

- No comprehensive data protection law
- New Cyber Security law passed in 2017
- Current law sanctions
- No DPO-like appointment required; changing?
- Current law requires some notification for data breach; timeline?

India Personal Data Protection Bill (PDP)

The PDP Bill is GDPR "Plus"

- Has not yet passed and is subject to change
- Includes strong personal privacy rights, broader scope, extra-territorial application, and high penalties for violations (up to $2.2 million or 4 percent of total gross revenue)
- Applies to processing of Personal Data collected by Indian companies within India, and to companies outside of India if the data processing takes place in India
- The Central Government of India *may* exempt outsourcing contracts from the law
- Consent is the primary ground for processing and has very few exceptions
- Includes a data localization provision that requires copies of Indian personal data be stored in India. It erects barriers that make it difficult to transfer sensitive or critical personal data out of India and requires express consent of the data subject.

Timing?

Global Privacy Law Highlights

The Philippines (PDPA)

- The PDPA is intended to comport with EU data privacy directive and subsequent GDPR; some of this is achieved through implemented rules. Key requirements include:
- 72-hour TAT for breach notification
- DPO designation required
- Robust Individual Rights
- Registration requirements for data processing
- Where consent required, consent is time bound
- Potential civil, administrative, or criminal penalties may be imposed for violations of the PDPA; violators of act could be banned from processing personal data
- Extraterritoriality but with limits; act applies to Philippine citizen or a resident

California (CCPA)

- California enacted the California Consumer Privacy Act of 2018 on June 28, 2018. The law is effective January 1, 2020.
- The CCPA Provides rights for California residents concerning Personal Information (PI) held by businesses. Consumers can:
  - Request businesses provide access to PI; disclose what PI is used for and to whom businesses share or sell PI;
  - Request deletion of PI held by businesses; and
  - Prohibit the sale of their PI.
- Consumers have a private right of action; damages of $100-$750 per consumer per incident or actual damages.
- Potential civil penalties of up to $2,500 for unintentional violations and $7,500 for intentional violations, per violation.
- HIPAA Covered Entities and Banks are exempt from the CCPA, but the extent of the exemptions are unclear.

Consider Cultural Differences

Our Background: Sectoral Based Privacy Laws; some state laws; no Federal Privacy Law

- Some countries are going from no cultural concept of privacy to mature European-style privacy laws without
- Trade Union importance in Europe
- History, Culture, and even Faith may inform concepts of privacy (KSA example)

Don't underestimate cultural differences when planning training and communication re: New Privacy Laws

What works in Minnesota may not work in Ireland or Brazil
Consider what each audience may need
Tailor training to audience

Consider desk drop communication with chocolate….

Consider Cultural Differences: Examples of Cultural Pitfalls

Said	Meant
So, this all looks good, but…	*Please rewrite completely*
Very interesting	*That's nonsense*
I'll get right on that	*I'll never finish this*
I guess that might be… OK	*I don't agree at all*
Well, that's different	*You are insane*
Maybe you should think about….	*Drop everything, do this*

Said	***Meant***
I only have a few minor comments	*Please re-write completely*
Very interesting	*That's nonsense*
Another cup of tea?	*Give me more time*
I almost agree	*I don't agree at all*
That's a brave proposal	*You are insane*
I hear what you say	*I disagree*

Q&A

Thank you!