RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **IDP-F02V**

Privacy: Fundamental right? Standards: Fundamental Requirement

John Britton

Senior Program Manager
Standards, Engineering Compliance,
Google

Laura Lindsay

Cybersecurity Standards Specialist
Corporate Standards Group,
Microsoft

After This Session

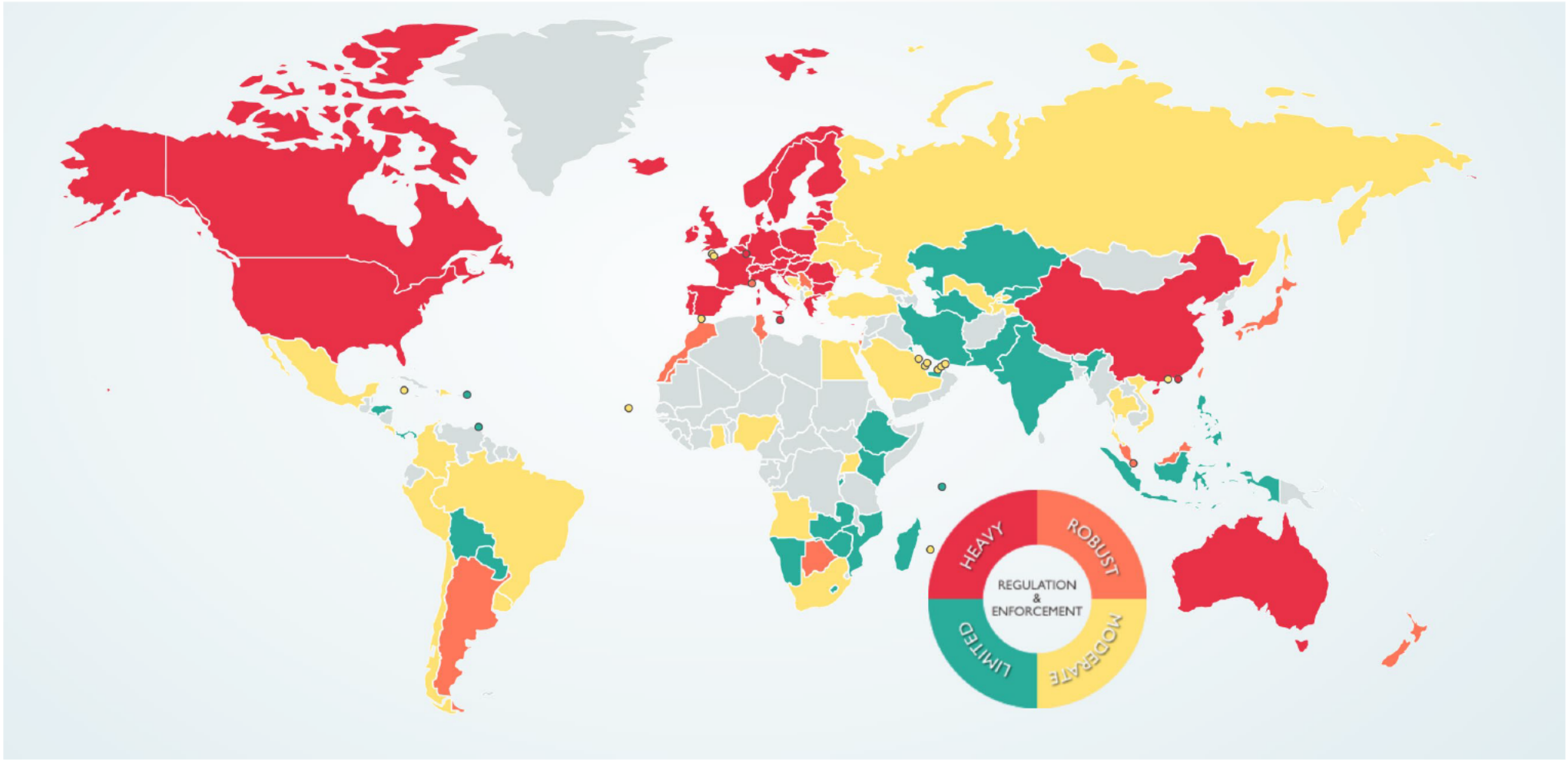
- Is your Organization impacted by privacy governance?
- Identify which Privacy governance models impact your organization.
- Choose the privacy governance model that works for your organization.
- Participate in standards development.

Why an ISO Standard ?

- Privacy is a challenging topic and depending on where you live, operate and travel governing bodies may have differing opinions on the answer to “Is Privacy a fundamental human right?”
- There are a variety of different existing regulations globally
- Compliance is necessary based on your business.
- How can you look at global requirements in a systematic and standard way?

An International Standard is a consensus driven way to do this.

Privacy Standard Globally



https://www.dlapiperdataprotection.com/

Global Market Needs Global Solution

Using the current jurisdiction-by-jurisdiction model of accountability is inefficient – making it more difficult for smaller companies to compete with bigger companies

In addition, use of ISO standards, by definition, adheres to WTO TBT rules

Use of ISO/IEC 27701, because of its flexibility, potentially solves this problem.

RSAConference2020 APJ

A Virtual Learning Experience

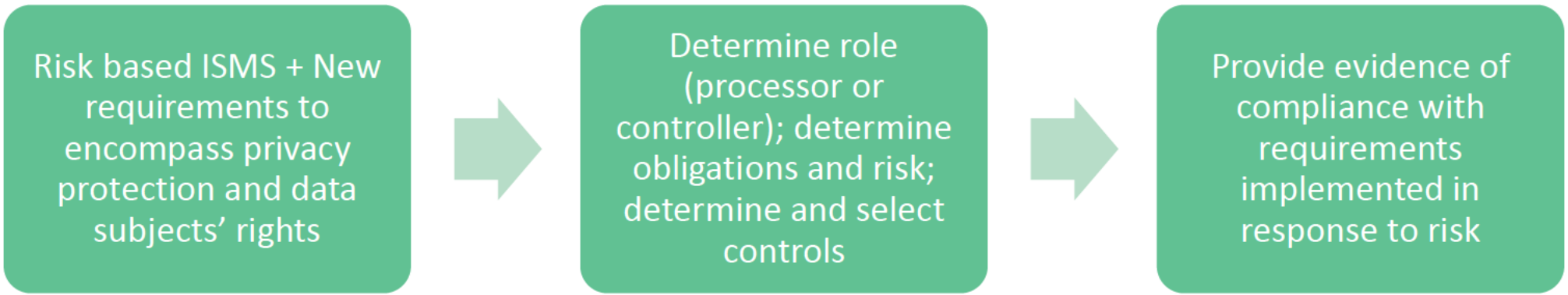
Why this ISO/IEC Privacy Standard?

Why Extend ISO/IEC 27001 for Privacy and why does it matter?

In Theory	ISMS as defined by ISO/IEC 27001 could be sufficient; scope *should* take into account regulations/laws and account for privacy requirements along with other regulatory, contractual, customer, etc. requirements
In Practice	Data protection law and other privacy regulations are complex and benefit from sector-specific guidance to satisfy both consumers and regulators
It Matters Because	With increasing privacy regulations across the world, a "privacy management system" standard and certification mechanism will provide a flexible baseline for meeting these expectations

What is ISO/IEC 27701?

- A standard that is an extension of ISO/IEC 27001 to encompass privacy concerns and protection of personal data (Privacy Information Management System)
- Does not replace 27001 or reproduce 27018, but allows organizations to integrate privacy considerations into their existing ISMS, whether a controller or a processor



History of ISO/IEC 27701

- Introduced by French DPA (CNIL) in ISO SC27
- 3 years in the making
- Expands on 27001 ISMS to more fully integrate privacy
- 27001 (PIMS) is a new management system standard with privacy requirements (new) as well as controls/guidance for both processors and controllers
- Certification standard, like ISO 27001, with the same ecosystem of auditors, accreditation bodies and certificates

ISO/IEC 27701

- A new standard that is an extension of ISO/IEC 27001 to encompass privacy concerns and protection of personal data (Privacy Information Management System)
- Does not replace 27001 or reproduce 27018, but allows organizations to integrate privacy considerations into their existing ISMS, whether a controller or a processor

Benefits to Organizations

- PIMS integrates with existing ISMS implementations
- Potential for one audit that satisfies multiple privacy regulations
- Help establishment of privacy best practices and evidence generation across the organisation
- Common industry baseline for privacy certifications

RSAConference2020 APJ

A Virtual Learning Experience

Using ISO/IEC 27701

ISO 27701 Structure

1 **Scope** — Discipline specific

2 **Normative Reference** — Discipline specific

3 **Terms and Definitions** — Discipline specific

4 **General**
- 4.1 Structure of the document
- 4.2 Application of ISO/IEC 27001:2013 requirements
- 4.3 Application of ISO/IEC 27002:2013 guidelines
- 4.4 Customer

5 **PIMS-specific 27001 requirements**
- 5.1 General
- 5.2 Content of the organization
- 5.3 Leadership
- 5.4 Planning
- 5.5 Support
- 5.6 Operation
- 5.7 Performance evaluation
- 5.8 Improvement

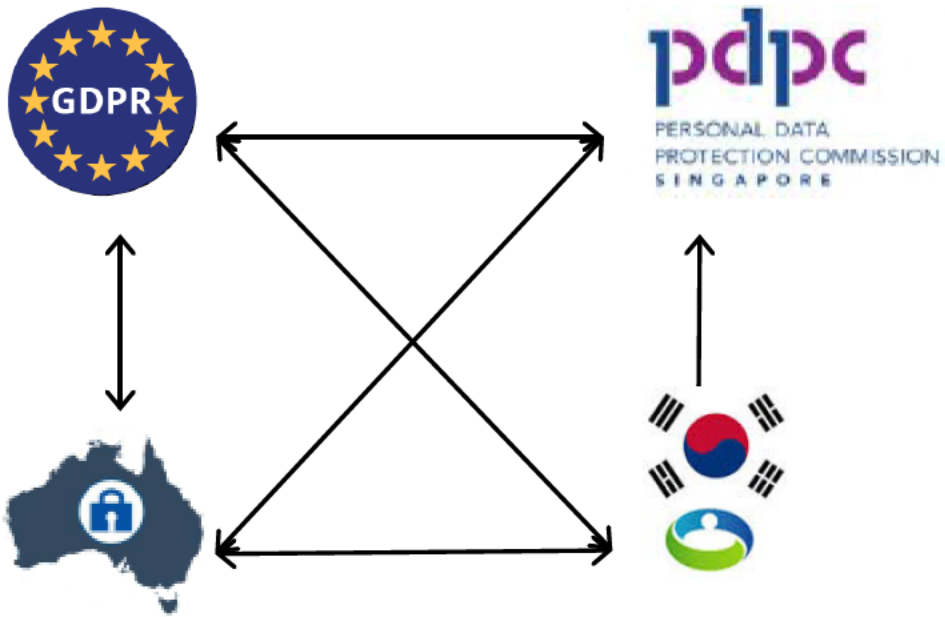
6 **PIMS-specific 27002 requirements**
- 6.1 General
- 6.2 Information security policies
- 6.3 Organization of information security
- 6.4 Human resource ability
- 6.5 Asset Management
- 6.6 Access Controls
- 6.7 Cryptography
- 6.8 Physical and environmental security
- 6.9 Operations Security
- 6.10 Communications security
- 6.11 Systems acquisitions, development, and maintenance
- 6.12 Supplier relationships
- 6.13 Information security incident management
- 6.14 Information security aspects of business continuity
- 6.15 Compliance

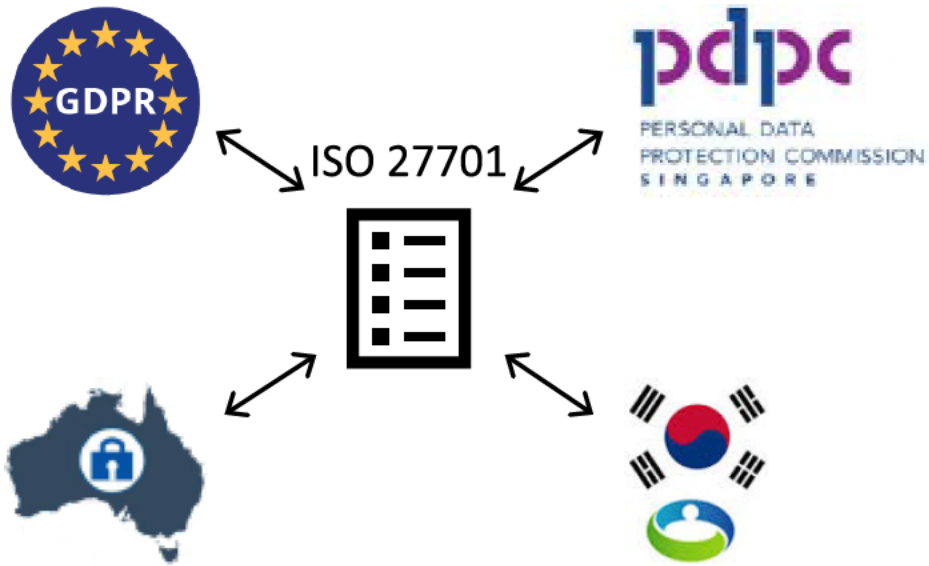
7 **27002 guidance for PII controllers**
- 7.1 General
- 7.2 Conditions for collection and processing
- 7.3 Obligations to PII principals
- 7.4 Privacy by design and privacy by default
- 7.5 PII Sharing, transfer, and disclosure

8 **27002 guidance for PII processors**
- 8.1 General
- 8.2 Conditions for collection and processing
- 8.3 Obligations to PI principals
- 8.4 Privacy by design and privacy by default
- 8.5 PII sharing, transfer, and disclosure

Required

Ease of comparing controllers and processors portions of regulations





Mapping Example

GDPR

Article 5 Principles relating to processing of personal data

1 Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')

ISO 27701

7.4.1 The [controller] should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.

7.4.4 The [controller] should define and document data minimization objectives and how those objectives are met, including what mechanisms (such as de-identification) are used

7.4.5 The [controller] should either delete PII or render it in a form which does not permit (re-)identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s)

7.4.6 The [controller] should ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.

8.4.1 The [processor] should ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period

PDPO

Principle 1—purpose and manner of collection of personal data

Principle 2—accuracy and duration of retention of personal data

26- Erasure of personal data no longer required

https://dataprotectionmapping.z21.web.core.windows.net/#/dashboard

Apply What You Have Learned Today

- Next week you should:
  - Determine if your organization is impacted by privacy governance?
- In the first three months following this presentation you should:
  - Identify which Privacy governance models impact your organization.
  - Choose the privacy governance model that works for your organization.
- Within six months you should:
  - Participate in standards development.

Thank you