



INTERNATIONAL  
**TRADE**  
ADMINISTRATION

# International Implementation of the APEC Privacy Framework

# Challenges to International Data Privacy Protection

- The International Organization for Standardization has noted that “the increased commercial use (and value) of PII, the sharing of PII across legal jurisdictions, and the growing complexity of ICT systems, makes it extremely difficult for an organization to ensure privacy and to achieve compliance with various laws and regulations.”
- Recognizing this challenge, member economies in the Asia Pacific Economic Cooperation’s (APEC) Electronic Commerce Steering Group (ECSG) developed the APEC Privacy Framework
- This Framework was endorsed by the Leaders of all 21 APEC member economies in 2004

# The APEC Privacy Framework

- Based on the 1980 OECD Guidelines, the Framework is an effort to bridge the various approaches to protecting the personal data collected in electronic transactions within the jurisdictions of APEC member economies
- The Framework is a set of nine principles to assist APEC economies in developing privacy approaches that maximize privacy protection and the continuity of cross-border information flows

# The APEC Privacy Principles

- 1) Preventing Harm
- 2) Notice
- 3) Use
- 4) Collection Limitation
- 5) Choice
- 6) Security Safeguards
- 7) Integrity
- 8) Access and Correction
- 9) Accountability

# The Role of Cross Border Privacy Rules

- Annex B of the Framework states that international implementation may be achieved through use of a voluntary system of Cross Border Privacy Rules (CBPRs)
- CBPRs are a set of rules developed by an organization based upon the APEC Privacy Principles
- An organization may voluntarily commit to apply these rules to its activities involving international transfers of PII across the APEC region
- Once an organization has opted to commit to these rules, participating APEC member economies will enforce the promises made
- Under this proposed system, APEC economies are given flexibility to chose the most appropriate way in which to enforce these promises.

# A Four Step Approach

## Self-Assessment

Company self-assesses using an Intake Questionnaire



## Certification

Accountability Agent verifies the attestation



## Recognition

Certification is published



## Enforcement

(Both internal through dispute resolution, external through regulation)

# The APEC Data Privacy Intake Questionnaire

- Purpose is to allow a company to map their privacy policies against the APEC Privacy Framework
- Developed over the last year by participating APEC Economies in the APEC Data Privacy Project 1 working group
- Endorsed at the most recent APEC Meeting in Sendai, Japan

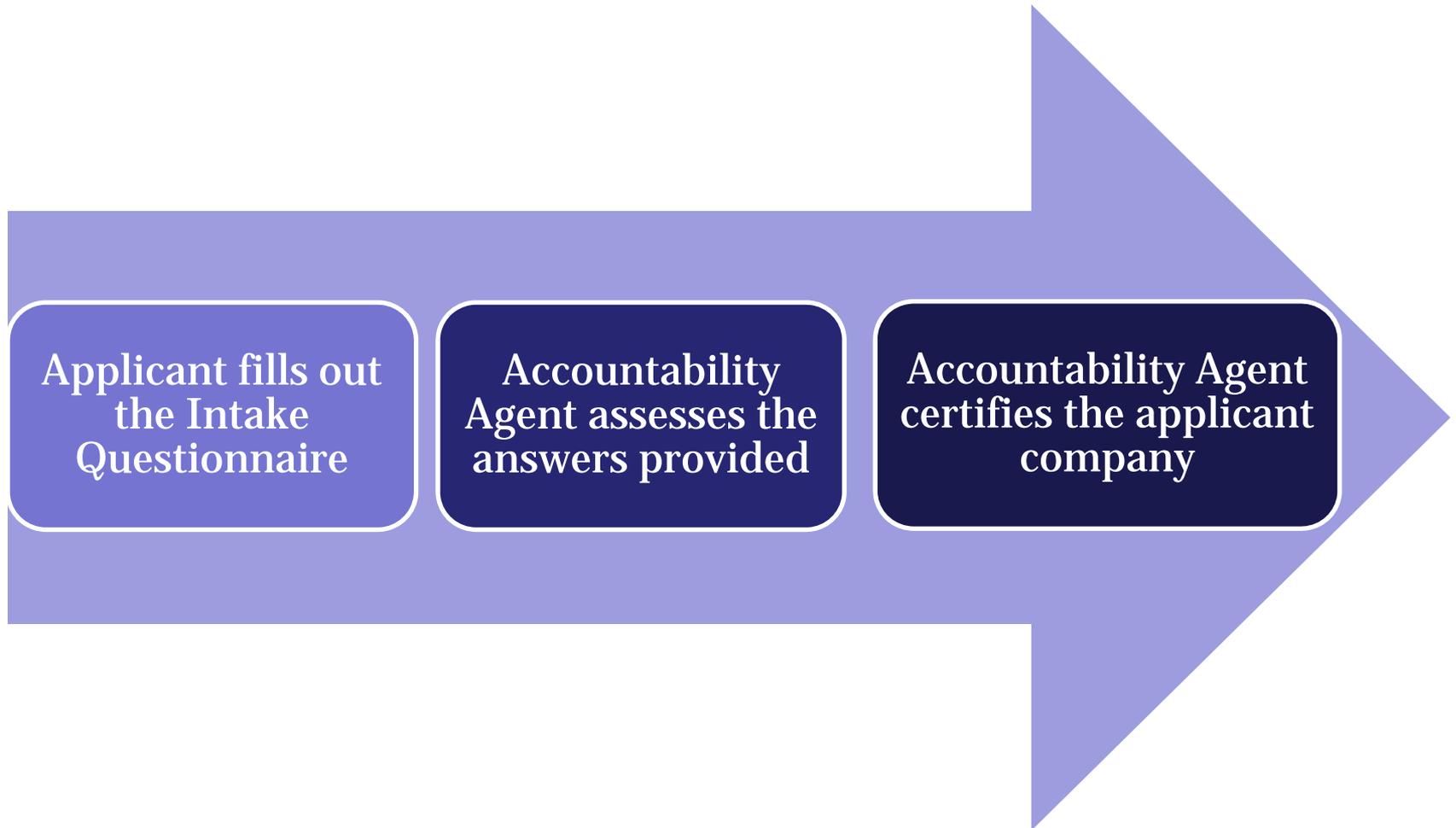
# The APEC Data Privacy Intake Questionnaire

- Consists of 51 questions
- Based on the APEC Privacy Framework
- Comprised of several sections, each corresponding to a specific APEC Privacy Principle (*e.g., Notice, Choice, Access and Correction* etc.)

# Assessing the Completed Questionnaire

- Questionnaire assessed by a third party, also known as an Accountability Agent, to verify accuracy
- Accountability Agent also assesses practices to ensure the identified policies are being implemented
- Applicant will be guided by program requirements that explain Accountability Agent's expectations as they relate to applicant's practices for each of the questions in the intake document
- Upon successful review, company's privacy policy will be 'APEC Certified'

# APEC Certification: Process Overview



# The APEC Enforcement Cooperation Arrangement

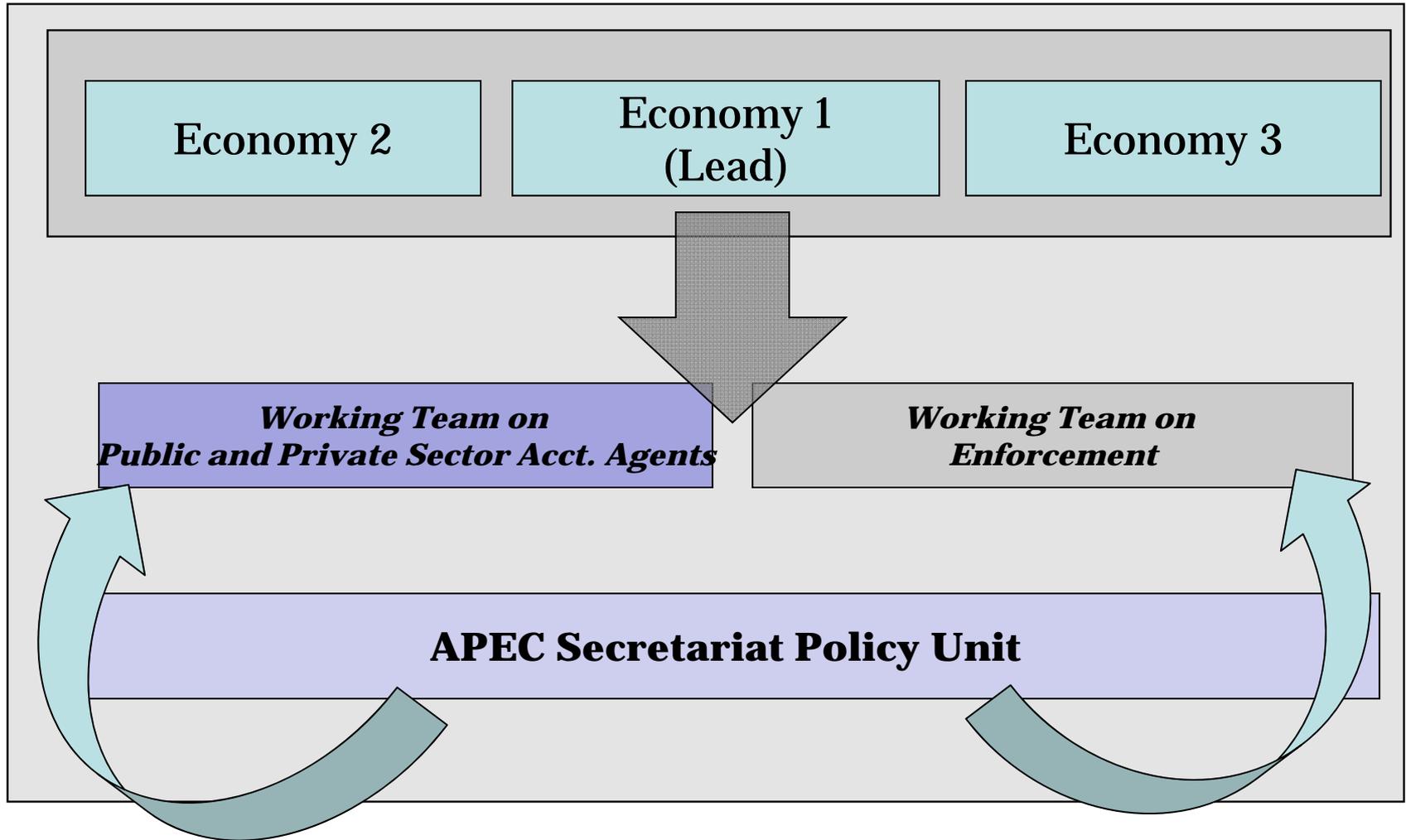
- Formally launched in July, 2010. Signatories include: Australia; Canada; Hong Kong, China; New Zealand and; the United States
- Privacy Enforcement Authority subscribes by giving written notice
- Must be supported by a letter of confirmation from the economy's ECSG delegation
  - **Privacy Enforcement Authority:** any public body responsible for enforcing Privacy Law
  - **Privacy Law:** laws that have the effect of protecting personal information consistent with the APEC Privacy Framework

# Next Steps: Governance

•Scope and Governance Document (in draft), requires development, including:

1. a glossary of terms;
2. a regulatory response pyramid (including complaint escalation);
3. funding options;
4. technological options to assist organizations in initial self-assessment
5. clarification of the relationship between Accountability Agents and privacy enforcement agencies ;
6. education and outreach;
7. an Accountability Agent MOU.

# CBPR Joint Oversight Committee (Proposed)



# BCRs and CBPRs: Application Comparison

## BCR Approval

- Applicant submits policies and practices for treatment of personal data for approval by the designated Approving Authority
- Lead Authority convenes a panel of member state authorities to review submission against external standard (Article 29 Working Party's guidance)

## CBPR Approval (*Proposed*)

- Applicant submits policies and practices for treatment of personal data for approval by a certified Accountability Agent
- Accountability Agent reviews submission against external standard (APEC Privacy Framework and related)

# BCRs and CBPRs: Scope Comparison

## BCR Scope

- After certification, entity may internally transfer to any covered entity within their listed corporate structure in all specified jurisdictions
- Third-party transfers require the use of standard contractual clauses as specified by the EU Commission (to be approved *prior to transfer*)

## CBPR Scope (Proposed)

- After certification, entity may transfer internally *and* externally (third-party transfers)
- Certified transfers limited to participating APEC jurisdictions

# BCRs and CBPRs: Enforcement Comparison

## BCR Enforcement

- Enforceable under EU Directive on data protection
- EU Directive is directly transposed into national data protection laws in member states
- Certified entity agrees to jurisdiction in all countries approved as part of its BCR

## CBPR Enforcement (*proposed*)

- Certified transfers limited to CPEA signatory economies
- Signatories must be able to enforce CBPRs but no specified legal mechanism
- Certified entity agrees to jurisdiction in all economies as part of the certified transfer

# International Implementation of the Framework: 2005-2012

- **2005:** APEC member economies formed a Cross Border Privacy Rules Study Group to study this approach
- **2007:** The *Data Privacy Pathfinder* is introduced
- **2008:** A work plan detailing nine voluntary projects necessary to implement the Pathfinder is introduced and endorsed
- **2009:** A CBPR Test Pilot is conducted across four economies
- **2010:** Six of the nine projects are completed and endorsed
- **2011:** Final endorsement, all projects completed (*Projected*)
- **2012:** Cross Border Privacy Rules System goes live (*Projected*)



INTERNATIONAL  
**TRADE**  
ADMINISTRATION

**Next SOM and Related APEC Meetings:**

**February 27-March 14, 2011,  
Washington, D.C.**