



# **CROSS-BORDER PRIVACY RULES Certification Process: A US Accountability-Agent Perspective**

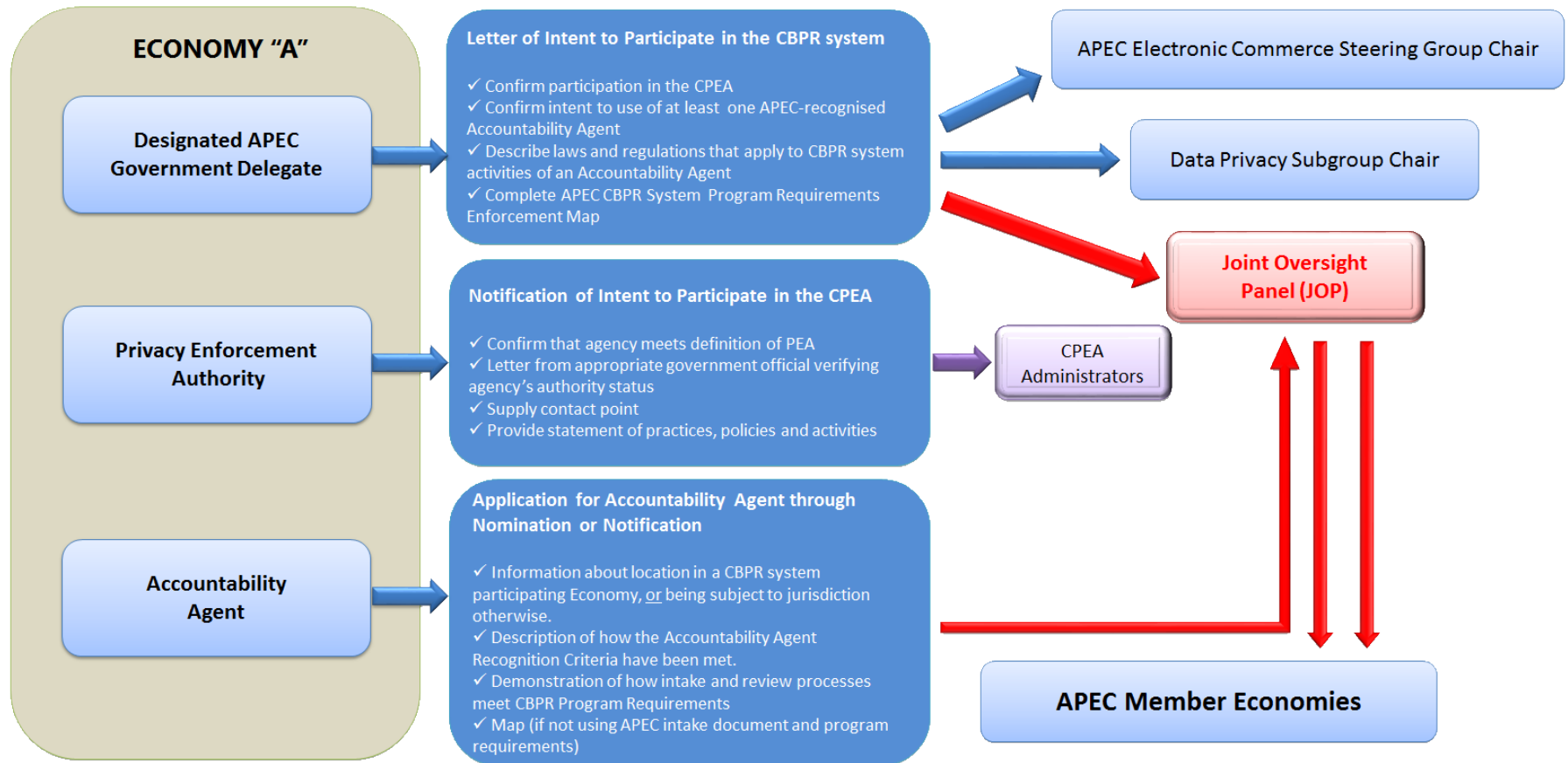
**Josh Harris**

**TRUSTe**

**Powering Privacy Compliance and Trust**

# Structure of the CBPR System

## Structure of the APEC Cross Border Privacy Rules (CBPR) system



# Accountability Agent Review Process

Category/Section	Description	Assigned to	No. of Questions
PSM Scoping	The following questions are part of the PSM's initial investigation and scoping review. Please review for accuracy.	Default	23
Introductory Questions		Default	9
Notice	<p>The questions in this section are directed towards:</p> <p>(a) ensuring that individuals understand your policies regarding personal information that is collected about them, to whom it may be transferred and for what purpose it may be used; AND</p> <p>(b) ensuring that, subject to the qualifications listed in part II, individuals know when personal information is collected about them, to whom it may be transferred and for what purpose it may be used.</p>	Default	10
Collection Limitation	The questions in this section are directed towards ensuring that collection of information is limited to the stated purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.	Default	3
Uses of Personal Information	The questions in this section are directed toward ensuring that the use of personal information is limited to fulfilling the purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that organization.	Default	4

# Example of Initial Attestation Form

## and Correction

Question	Answer Type
Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual?	YES_NO
Upon request, do you provide individuals access to the personal information that you hold about them?	YES_NO
Do you provide access within a reasonable timeframe following an individual's request for access?	YES_NO
Is information communicated in a reasonable manner that is generally understandable (in a legible format)?	YES_NO
Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?	YES_NO
Do you charge a fee for providing access?	YES_NO
Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted?	YES_NO

re

Publish Assessment

← Security Safeguards

Accountab

# Remediation Process



## b. Required Changes

The following changes are required to complete certification and to display the TRUSTe seal.

<b>Review Findings #1:</b>	
<b>Finding:</b>	
<b>Required Change:</b>	
<b>Resolution:</b> <u>Pending</u> /Yes	<b>Date Resolved:</b>
	<b>Resolved by:</b>
<b>Review Findings #2:</b>	
<b>Finding:</b>	
<b>Required Change:</b>	
<b>Resolution:</b> <u>Pending</u> /Yes	<b>Date Resolved:</b>
	<b>Resolved by:</b>
<b>Review Findings #3:</b>	
<b>Finding:</b>	

# Status of APEC-Art. 29 Interoperability Project

---

## **Creation of Joint EU-APEC Working Team:**

- Recognized value of collaboration to provide industry greater clarity on how to meet requirements of EU and APEC simultaneously

## **Development of “Referential”:**

- Mapped requirements of APEC CBPR System and EU BCR System
- Identified common and divergent elements to help inform companies seeking to develop policies and practices in compliance with both systems
- APEC Data Privacy Subgroup expression of interest to Article 29 Working Party regarding tools recommended by joint working team in January 2015

## **Next Steps:**

- Work together to develop practical tools to facilitate dual certification to complement referential: Meetings held in most recently in Amsterdam, discussions to continue at APEC 2016 in Peru.

# Current Companies (As of October, 2016)

---

- Adaptive Insights
- Apple
- Box
- Cisco
- Hewlett Packard Enterprise
- Hightail
- HP Inc
- IBM
- Lynda.com
- Mashable
- Merck
- Rimini Street
- Saba Software
- The Ultimate Software Group
- Workday
- Yodlee
- Ziff Davis



**Josh Harris**

[jharris@truste.com](mailto:jharris@truste.com)

Powering Privacy Compliance and Trust