Asia-Pacific
Economic Cooperation

2013/SOM1/ECSG/DPS/I/002
Agenda Item: II

CBPR Intake Document

Purpose: Information
Submitted by: United States

Data Privacy Subgroup Informal Meeting
Jakarta, Indonesia
31 January 2013

APEC CROSS-BORDER PRIVACY RULES SYSTEM
INTAKE QUESTIONNAIRE FOR DATA PROCESSORS

This document is intended to assess the ability of a data processor to understand and help the personal information controller for whom they provide services meet their privacy obligations. The controller is the party that makes decisions on the data to be collected and the purposes for which the data will be used. It is also the controller that makes commitments to individuals. The processor must be able to understand those commitments and have the ability based on instructions from the controller to assure they are fulfilled. For a processor to receive recognition of its processor cross border privacy rules it must demonstrate a set of policies and practices that create confidence that it will meet its obligation to the controller and the individuals served by that controller. A certified processor will be held accountable for the policies and practices listed in this assessment by an accountability agent. This survey is based on recent direction on the elements of a comprehensive privacy program.

Organizational Commitment

Senior Management Commitment

1) Does your organization have in place mechanisms, such as high level policies endorsed by a senior executive or a governance structure for privacy protection that reports to senior management, to assure senior management has endorsed your organization's comprehensive privacy program?

2) Does senior management review regularly the resources allocated to privacy protection and make appropriate adjustments commensurate with the nature and sensitivity of personal information that the organization is entrusted for processing by their clients?

3) Does senior management communicate its policy endorsement to employees?

Privacy Executive and Supporting Team

4) Is there a process in place to ensure that privacy protection is considered in business decision making?

5) Are the roles and responsibilities of the personnel for monitoring compliance clearly identified?

6) Is there a process that exists to determine necessary resources (resources for what?) and is this process linked (what is the significance of this linkage?) to changing business needs?

7) Is the privacy organization's purpose (What is the meaning of privacy organization? Does it mean a privacy team?), responsibility and authority communicated throughout the relevant parts of the organization?

8) Is the privacy organization (What is the meaning of privacy organization? Does it mean a privacy team?) responsible for the development and implementation of the program and its ongoing assessment and revision, including privacy assessments and implementation? (What is the point of asking this question? Would it be a better answer if the responsibility is owned by senior staff at the top and shared by other teams as well?)

9) Is privacy protection built into every major function involving the processing of personal information?

Reporting

10) Are reporting mechanisms clearly defined and reflect your organization's program controls?

11) Are processes in place to escalate privacy related issues to senior levels?

Implementation Controls and Procedures

12) Does the organization have a process for turning client determined requirements on privacy protection into processing controls?

Policies

13) If your organization interfaces directly with a client's customers, does your organization have a means of getting clear direction from the client based on the client's policies as they relate to:

    a) Collection, use and disclosure of personal information, which include requirements for consent and notification;

    b) Defined process for assessing the risk to individuals to assure fair processing when consent is inappropriate or not possible; (What does this entail?)

       (What about data retention? and further subcontracting?)

    c) Access to and correction of personal information;

    d) Redress for individuals with complaints and concerns;

    e) Data and physical security proportional to the risks to individuals

Training and Education Requirements

14) Does your organization have documented programs to train employees to understand the organization's policies and procedures with regard to privacy protection?

15) Are employees trained to the level necessary to assure they observe the privacy requirements?

Breach and Incident Management Response Protocols

16) Does your organization have processes that exist for identifying data breaches and alerting the client to those breaches, and for facilitating the forensics necessary to isolate the cause, risks and remedies of any data breach?

Client Management

17) Is Privacy an element of contract negotiations (with whom?)?

18) Do contracts (with whom?) contain provisions related to privacy?

Security Safeguards

19) Has the organization implemented an information security policy that covers the client data?

20) Do you (It is necessary to be consistent throughout the questionnaire to use either "you" or "your organization".) have programs to maintain the physical, technical and administrative safeguards specified by the client?

21) Describe how you make your employees aware of the importance of maintaining the security of personal information.

22) Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:

    a) Employee training and management or other organizational safeguards?

    b) Information systems and management, including network and software design as well as information processing, storage, transmission, and disposal?

    c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?

    d) Physical security?

23) Have you implemented a policy for the secure disposal of personal data based on instructions from a client?

24) Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?

25) Do you have processes in place to test the effectiveness of the safeguards referred to in the question above?

26) Do you use third-party certifications or other risk assessments? Please describe.

27) Do you require subcontractors to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:

    a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?

b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of your organization's personal information?

c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?

(Suggest to include the following questions:-

Commitments to Clients

1, Has the organization implemented policies and practices not to use personal information entrusted by clients for any purpose other than those specified by the client?

2. Has the organization established policies and practices to return (or permanently destroy if appropriate) personal information entrusted by client after completion of the task engaged by client?

3. Has the organization established policies and practices to comply with the client's instruction to keep personal information only in specified locations and/or jurisdictions?

Accountability

28) What measure does your organization take to ensure compliance with the APEC Information Privacy Principles that are related to the activities of data processing? Please check all that apply and describe.

a) Internal guidelines or policies (if applicable, describe how implanted)

b) Compliance with applicable industry or sector laws and regulations

c) Compliance with self-regulatory organization code and/or rules

d) Other (describe)

29) Has your organization appointed an individual(s) to be responsible for your organization's overall compliance with the Privacy Principles?

30) Does your organization have procedures in place to investigate privacy-related complaints forwarded by clients?

31) Do you have procedures in place for responding to judicial or other government subpoenas, warrants or order, including those that require the disclosure of personal information?

32) Do you have mechanisms in place with subcontractors to ensure obligations from clients are honored?

33) Do these mechanisms generally require that subcontractors:

a) Follow-instructions provided by you relating to the manner in which your personal information must be handled?

b) Impose restriction on further subcontracting unless the organization seeks consent

c) Have their CBPRs certified by an APEC accountability agent in their jurisdiction?

d) Do you require your subcontractors to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If yes, describe.

e) Do you carry regular spot checking or monitoring of your subcontractors?

Oversight and Revision

34) Does your organization develop oversight and review plan? (Does it matter if somebody else (e.g. consultant) develop the plan?)

Assessment and Revision Controls

35) Where processing requirements set by the client are dynamic and changing, is there ongoing contact with the client to understand changes in processing and to document new risks to individuals identified by the client?

36) Are contracts revised to assure new obligations are met?