APEC CROSS-BORDER PRIVACY RULES SYSTEM
JOINT OVERSIGHT PANEL

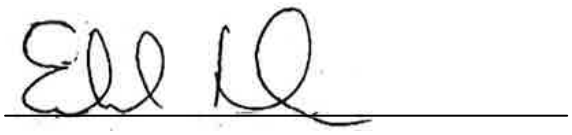
ADDENDUM TO THE RECOMMENDATION REPORT ON APEC RECOGNITION OF JIPDEC

Submitted To: Mr. Ted Dean
Chair, APEC Electronic Commerce Steering Group
8 January 2016

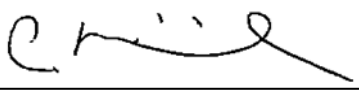
EXECUTIVE SUMMARY

On 18 August 2015, the APEC Cross Border Privacy Rules (herein 'CBPR') system's Joint Oversight Panel (herein 'JOP') circulated its recommendation to APEC member Economies regarding JIPDEC's application for APEC recognition to participate as an Accountability Agent in Japan as part of the CBPR system. In that report, the JOP concluded that in its opinion, JIPDEC had met each of the Recognition Criteria as identified in the APEC Accountability Agent Recognition Application. APEC member Economies were then asked to make a determination as to JIPDEC's request for recognition, taking into account the JOP's recommendation. To facilitate this deliberative process, paragraph 20 of the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel states that "any APEC member Economy may request additional information or clarification from the applicant Accountability Agent when making a determination on whether to grant the applicant Accountability Agent's request for recognition." Pursuant to this, Hong Kong, China has asked for clarification on a number of issues in the JIPDEC's application having undertaken domestic consultations. Following is additional information for Member Economy consideration regarding the issues provided by Hong Kong, China (herein "comments") as they pertain to identified recognition criteria.

Signed,



Ted Dean
Chair, Joint Oversight Panel, United States Department of Commerce



Colin Minihan
Co-Chair, Joint Oversight Panel, Attorney-General's Department, Australia

Shinji Kakuno
Co-Chair, Joint Oversight Panel, Ministry of Economy, Trade and Industry, Japan

8 January 2016

Paragraph 6.4 of the JOP Charter

In the comments, JOP was requested to clarify that paragraph 6.4 of the JOP Charter applies or not to apply to JIPDEC application. The JOP has confirmed that JIPDEC is not government entity and it became a general incorporate foundation which is stipulated in the Act on General Incorporated Association and General Incorporated Foundations on April 1 2011.Therefore, JOP concluded that paragraph 6.4 of the JOP Charter does not apply JIPDEC application.

Annex C Question 1(a) –JIPDEC's Program Requirement 3.5

The comments point out that paragraphs (3) (a) to (c) of the program requirement of JIPDEC (herein "program requirement") provide for wide exceptions to give notification to individuals. In its consultations with JIPDEC, they provide additional explanations on these issues as follows. Paragraphs (3) (a) to (c) is based on Article 18 of the Act on Personal information protection (herein "the Act"). Article 18 of the Act refers Individual Participation Principle of OECD Privacy Guideline. So program requirement 3.5 is premised on protection of the right of individuals and requires the applicant business entity to provide adequate measures for ensuring the right of individuals. For instance, paragraphs (3) (a) applies that informing the purpose of using some kind of personal information to a person causes him/her understood the name of disease (psychological damage) and how it would be difficult to care the disease in the hospital. In addition, "other rights or interest" is basket clause for protecting other rights of individuals which should be given priority over informing the purpose of using the information. Paragraphs (3) (b) applies the situation that commercial secrets or new products and services under developing will be disclosed by revelation of purpose of using personal information. Paragraphs (3) (c) applies the situation that personal information of a suspect should be informed of police and court for criminal investigation.

Annex C Question 6 –JIPDEC's Program Requirement 3.1 and 3.6

The comments pointed out that program requirement 3.1 and 3.6 both relate to the "use" rather than "collection" of personal information. In its consultation with JIPDEC, they provide additional explanations on the issue. Program Requirement 3.1 and 3.6 are based on program requirement 2.1 which requires the applicant business entity to make and maintain records including "Each type of data collected", "The corresponding stated purpose of collection for each", "All uses that apply to each type of data", "An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection" and "review process the purpose of collection". Program Requirement 2.1 represents legal requirements of Article 15 and Article 16 of the Act. Article 15 of the Act requires that business entity shall specify the purpose of utilization of personal information and not to change the purpose of utilization beyond the scope which is reasonably considered that the purpose of utilization after the change is duly related to that before the change. Article 16 of the Act requires that business entity shall not handle personal information about the person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the purpose of

utilization specified pursuant to the Article 15. So JIPDEC modified Relevant Program Requirement column of Question 6 in Annex C to add program requirement 2.1.

Annex C Question 6 –JIPDEC's Program Requirement 3.6 (4) (c)

The comments request elaboration and provision of real examples on 3.6 (4) (c). JIPDEC provides additional explanation on the request. Program requirement 3.6 is based on Article 16 of the Act. Article 16 concretizes Use Limitation Principle of OECD Privacy Guideline and stipulates that the business entity must not use personal information beyond the scope of purpose of use except for some cases. Program requirement 3.6 (4) (c) is one of exemptions for improvement of public hygiene or promotion of the sound growth of children. For instance, epidemiological survey for prevention of disease and other follow up surveys, and cooperation among relevant regional administrators and local communities for prevention of delinquency are included in this program requirement.

Annex C Question 6 –JIPDEC's Program Requirement 3.6 (4) (d)

The comments point out that program requirement 3.6 (4) (d) appears too wide. Hong Kong states that not all government activities will justify a blanket exemption from the use requirement. In its consultation with JIPDEC, they assure exemption from the use requirement is limited only when it is necessary to cooperate with state or local government in executing the affairs prescribed by laws and regulations and in which notifying the person of the purpose of utilization is likely to impede the execution of the affairs. As explained in program requirement 3.5 (3) (c), it applies the situation that personal information of a suspect should be informed of police and court for criminal investigation.

Annex C Question 17-19 –JIPDEC's Program Requirement 1.2, 3.4, 3.8 and 5.2

The comments point out that program requirement 1.2, 3.4, 3.8 and 5.2 do not fully cover whether Applicant's choice mechanism is displayed or provided in a clear and conspicuous manner, is clearly worded and easily understandable and is easily assessable and affordable. In its consultation with JIPDEC, they provide additional explanation on this issue. Firstly, the applicant should obtain consent from individuals. In addition, individuals have the rights of disclosure, correct, add, delete, stop using, erase and stop providing to a third party based on program requirement 5.1. So JIPDEC modified Relevant Program Requirement column of Question 17-19 in Annex C to add program requirement 5.1.

Annex C Question 23 –JIPDEC's Program Requirement 4.1 and 4.4

The comments point out that program requirement 4.1 and 4.4 do not describe directly requirement on communication to have processors, agents or other service providers correct personal information. In its consultation with JIPDEC, they confirm that program requirement 4.1 applied to the processors, agents or other service providers, and the applicant have to supervise them under program requirement 4.4 for the correction of personal information of their possession.

Annex C Question 29 –JIPDEC's Program Requirement 2.3, 4.2, 4.3 and 6

The comments request whether the employees are required to sign the information security policy because JIPDEC program requirement 4.3(2) requires the applicant to sign a non-disclosure agreement with respect to personal information with its employees. In Japan, making a contract of non-disclosure agreement with its employees means that he or she makes a commitment under the Civil Code to keep confidentiality of any information assets of the organization including personal information. It is a case-by-case basis whether the term, "Information Security Policy", specifically is written in the agreement.

Annex C Question 30(b) and (c) –JIPDEC's Program Requirement 2.3, 4.2, 4.3 and 6

The comments point out that Question 30 (b) and (c) ask the organization to implement safeguards in information system and management, including network and software design and to prevent attacks, intrusion, or other security failures but program requirement 2.3, 4.2,4.3 and 6 do not answer specifically. In its consultation with JIPDEC, they confirm program requirement 4.2 includes measures for network protection, detecting and preventing attacks, intrusion, or other security failures as part of requirements on 4.2(5), 4.2(6) and 4.2(8).

Annex C Question 32 and 33 –JIPDEC's Program Requirement 2.3 and 4.2

The comments point out that program requirement 2.3 and 4.2 do not relate to Question 32 and 33. Regarding this comment, JIPDEC states that Question 32 stipulates measures to detect, prevent and respond to attacks, intrusions or other security failures. This means such attacks and intrusions are already known. Program requirement 2.7 applies when the organization is attacked by unknown virus e-mail. They think that Question 32 and 33 are covered by program requirement 4.2 (5) to (8).

Annex C Question 35 –JIPDEC's Program Requirement 2.3, 2.7, 4.2, 4.3 and 4.4

The comments point out that program requirement 2.3, 2.7, 4.2, 4.3 and 4.4 do not fully cover all matters stipulated in Question 35. In its consultation with JIPDEC, they assure all matters are covered by program requirement 4.4. The applicant shall supervise processors, agents, contractors or other service providers for protection against loss, unauthorized access, destruction, use, modification, disclosure or other misuses of the information. In addition, program requirement 4.4 is based on the Article 22 of the Act and this article states that the applicant has all responsibility on their business activities including business outsourcing.

Annex C Question 36 –JIPDEC's Program Requirement 5.2

The comments point out that Question 36 requires Accountability Agent to verify whether the applicant provides the individual with a time frame indicating when the requested access will be granted or not and the personal information must be provided in an easily comprehensible way, but JIPDEC cannot explain enough. In its consultation with JIPDEC, they modified their program requirement 5.1 and 5.2. Regarding program requirement 5.1, a clear time frame was added. It requests that the applicant to respond to requests from individuals including access to their information within one month in principle. In addition, the applicant has to prepare

the requested information in an easy to understand way under program requirement 5.2. If the applicant cannot reply the requested access within one month, it must inform the individual of the status and reason. So JIPDEC modified Relevant Program Requirement column of Question 36 in Annex C to add program requirement 5.1.

Annex C Question 37 and 37 (c) to (e) –JIPDEC's Program Requirement 5.2, 5.3, 5.5 and 5.7

The comments point out that program requirement 37 (a) and (b) are too wide as an exemption for not to provide individual access and 37 (c) to (e) do not fully cover all matters. In its consultation with JIPDEC, they explained this program requirement 37 (a) and (b) are applied in a limited extent in principle. In addition, they provide some examples. Program requirement 37(a) is applied that support organization for victims of domestic violence does not respond to the request from the assailant. Program requirement 37(b) is applied that company owns personal information in which an individual who complains repeatedly is the person in order to prevent the damage from unjustified demand by a so-called suspicious individual and a vicious complainer. Regarding program requirement 5.2 and 5.5, the applicant is required to establish a procedure including form of documentation such as an e-mail and other concrete measures, and a method for collecting charges as a condition of not imposing an excessive burden on the requesting individual.

Annex C Question 38(d) and (e) –JIPDEC's Program Requirement 5.1, 5.2, 5.3 and 5.6

Question 38(d) requests the applicant to provide a copy to the individual of the corrected personal information, and question 38(e) requests the applicant to provide an explanation to individuals when access and correction are refused. The comments request to clarify whether program requirement 5.1, 5.2, 5.3 and 5.6 provide such confirmation and explanation to individuals. In its consultation with JIPDEC, they provide additional information that program requirement 5.7 requests the applicant to notify individuals of their response to the request from an individual regarding stopping use etc. of personal information and to provide a copy on correction of personal information including deletion and amendment. So JIPDEC modified Relevant Program Requirement column of Question 38(d) and (e) in Annex C to add program requirement 5.7.

Annex C Question 43 –JIPDEC's Program Requirement 1.3 and 8

The comments point out that program requirement 1.3 and 8 do not fully explain the remedial action relating to complaints. In its consultation with JIPDEC, they confirm program requirement 1.3(5), 8(1) and (2) include the remedial action. In addition, handling of complaints is requested by the Article 31 of the Act and therefore the applicant have to set up contact point for handling complaints and to make procedure how to handle complaints.

Annex C Question 44 –JIPDEC's Program Requirement 6

The comments request to specify whether or not program requirement 6 includes how the applicant trains its employee with respect to privacy-related complaints. In its consultation with JIPDEC, they explained that employee education and training are implemented to make

employees understand necessary matters for each relevant function and level.

Annex C Question 45 –JIPDEC's Program Requirement 2.2, 2.5 and 6

The comments point out that program requirement 2.2 only requires the applicant to establish a procedure and management system for identifying and referring to law, guidelines and other codes stipulated by the government of Japan regarding the handling of personal information. There is no reference to "procedures in place for responding to judicial or other government subpoenas, warrants or orders including those that require the disclosure of personal information" under Question 45. In its consultation with JIPDEC, they modified their program requirement 2.2 and 2.2(4) as follows. "The applicant business entity shall establish a procedure and management system for identifying and referring to laws, guidelines, and other codes stipulated by the government of Japan regarding the handling of personal information including responding to judicial or other government subpoenas, warrants and orders." ,"Identified laws, guidelines, and other codes that need to be referenced are made available for reference as necessary and such references are required to include appropriate procedures to handle inquiries, requests, etc. from abroad."

Annex C Question 47 to 50 –JIPDEC's Program Requirement 4.4

The comments request to elaborate the explanation on each requirement in Question 47 to 50. In its consultation with JIPDEC, they modified the first sentence of their program requirement 4.4 as follows; "The applicant business entity, when entrusting handling of personal information, shall establish criteria for selecting trustees and select trustees who satisfy the requirements for the sufficient protection level that is the same as or higher than the protection level of the applicant business entity. (*The term "trustees" here includes processors, agents, contractors or other service providers who are entrusted to handle personal information.)"

Regarding Question 49, they provide additional explanation that program requirement 4.2 and 4.4(3) include spot monitoring as part of periodical reevaluation of trustees and other security control measures for personal information. So JIPDEC modified Relevant Program Requirement column of Question 46 to 49 in Annex C to add program requirement 4.2.