CROSS-BORDER PRIVACY RULES SYSTEM JOINT OVERSIGHT PANEL

RECOMMENDATON REPORT ON APEC RECOGNITION OF THE KOREA INTERNET AND SECURITY AGENCY (KISA)

Submitted to: Nicolas Schubert

Chair, Digital Economy Steering Group

November 26, 2019

TABLE OF CONTENTS

Executive Summary 1

Scope of Consultation Process 1

Recommendation of the Joint Oversight Panel 2

Request for Consensus Determination 3

Enforceability 4

Recognition Criteria 5

Conflicts of Interest (Recognition Criteria 1-3) 5

Program Requirements (Recognition Criterion 4) 6

Certification Process (Recognition Criterion 5) 6

On-going Monitoring and Compliance Review Processes (Recognition Criteria 6, 7) 7

Re-Certification and Annual Attestation (Recognition Criterion 8) 8

Dispute Resolution Process (Recognition Criteria 9, 10) 8

Mechanism for Enforcing Program Requirements (Recognition Criteria 11-15) 9

Case Notes & Statistics 11

Signature 12

EXECUTIVE SUMMARY

On June 7, 2017, the Republic of Korea formally commenced participation in the Cross Border Privacy Rules (hereinafter 'CBPR') System. Pursuant to Paragraph 5 of the Protocols of the Joint Oversight Panel, the Republic of Korea was then eligible to nominate one or more Accountability Agents for APEC recognition.

In December 2017, the Joint Oversight Panel (hereinafter 'JOP') received an application from Korea's Ministry of the Interior and Safety (hereinafter MOIS) and the Korea Communications Commission (hereinafter KCC) nominating the Korea Internet & Security Agency (hereinafter KISA) as an APEC Accountability Agent for the CBPR System. A revised application was submitted on July 17, 2019.

SCOPE OF CONSULTATION PROCESS

Pursuant to Paragraph 7.2 of the *Charter of the Joint Oversight Panel*, members of the JOP[1] began a consultative process with representatives from KISA to:

- Confirm the enforceability of an organization's CBPR obligations once certified as CBPR compliant by KISA;
- Confirm KISA's location and the relevant enforcement authority;
- Confirm that KISA meets the recognition criteria as identified in the *Accountability Agent Application for Recognition*;
- Confirm KISA makes use of program requirements that meet the baseline established in the CBPR System; and
- Confirm KISA has provided the necessary signature and contact information.

The following Recommendation Report was drafted by members of the JOP.

[1] Members of the JOP are: Shannon Coe, Department of Commerce, United States; Shuji Tamura, Ministry of Economy, Trade and Industry, Japan; and Evelyn Goh, Personal Data Protection Commission, Singapore.

RECOMMENDATION OF THE JOINT OVERSIGHT PANEL

Having verified that the Republic of Korea is a participant in the APEC Cross Border Privacy Rules (CBPR) System and has demonstrated the enforceability of the CBPR program requirements pursuant to the information provided in Annex B of the Republic of Korea's Notice of Intent to Participate;

Having verified that KISA is in the Republic of Korea and is subject to the oversight and enforcement authority described in Annex A of Korea's Notice of Intent to Participate;

Having verified with the Administrators of the APEC Cross Border Privacy Enforcement Arrangement (CPEA) that Korea's Ministry of the Interior and Safety (hereinafter MOIS) and the Korea Communications Commission (hereinafter KCC), Privacy Enforcement Authorities in the Republic of Korea, are participants in the APEC CPEA;

Having determined, in the opinion of the members of the Joint Oversight Panel, that KISA has policies in place that meet the established recognition criteria and makes use of program requirements that meet those established in the CBPR System, and;

Having verified KISA has provided the required signature and contact information;

The JOP recommends APEC Member Economies consider the conditions established in 7.2 (ii) of the Charter of the Joint Oversight Panel to have been met by KISA and to grant the Republic of Korea's request for APEC recognition of KISA to certify organizations within the Republic of Korea and under the jurisdiction of MOIS and KCC as compliant with the CBPR System pursuant to the established guidelines governing the operation of the CBPR System.

Submitted by the Joint Oversight Panel:

Shannon Coe
Chair, Joint Oversight Panel
U.S. Department of Commerce, United States

Evelyn Goh
Member, Joint Oversight Panel
Personal Data Protection Commission, Singapore

Shuji Tamura
Member, Joint Oversight Panel
Ministry of Economy, Trade and Industry, Japan

REQUEST FOR CONSENSUS DETERMINATION

APEC Member Economies are asked to make a determination as to the Republic of Korea's nomination and request for recognition of KISA as an Accountability Agent, taking into account the JOP's recommendation. Any APEC Member Economy has the right to reject the request of an applicant Accountability Agent for recognition for failure to meet any of the recognition criteria required in the *APEC Accountability Agent Recognition Application*. When making this determination, any APEC Member Economy may request additional information or clarification from the Republic of Korea or the JOP. If no objection is received within the deadline for consensus determination as established by the DESG Chair, the request will be considered to be approved by the DESG. Should Member Economies determine that KISA has met the necessary criteria, APEC recognition will be limited to one year from the date of recognition, one month prior to which, KISA may re-apply for APEC recognition if it so wishes, following the same process described herein.

I. ENFORCEABILITY

Is the Applicant subject to the jurisdiction of the relevant enforcement authority in a CBPR participating Economy?

Recommendation

The JOP is satisfied that KISA is subject to oversight and enforcement with respect to its certification activities in accordance with the CBPR System requirements.

Discussion

KISA is a special legal entity established under The Republic of Korean law[2] to perform business affairs related to personal information protection and operate the domestic personal data protection certification system. The JOP has confirmed that KISA is subject to oversight by both MOIS, the ministry in charge of matters concerning personal information protection handled by public institutions and offline business operators, and KCC, the ministry in charge of personal information protection handled by online business operators. Pursuant to Article 14 of the Regulation on Delegation and Entrustment of Administrative Authorities, KISA would be performing its duties as an Accountability Agent pursuant to the delegated authorities of MOIS and KCC. KISA would therefore be subject to the regulatory supervision of its delegated duties and the executive power of these ministries. The JOP has further confirmed that MOIS and KCC direct and supervise KISA, may give instructions or order KISA to take measures regarding the conduct of its duties as an Accountability Agent, and that they may cancel or suspend KISA's certification activities if KISA's conduct is deemed to be illegal or unfair.

[2] KISA is: 1) a special legal entity established according to paragraph 1 of Article 52 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., 2) a nonprofit corporation according to Article 32 of the Civil Act, and 3) a public institution according to Article 4 of the Act on the Management of Public Institutions.

II. RECOGNITION CRITERIA

The *Accountability Agent Application for Recognition* requires applicants to describe how each of the 15 Accountability Agent Recognition Criteria have been met using the Accountability Agent Recognition Criteria Checklist. Following is an overview of each listed requirement and recommendation of the sufficiency of each based on the information submitted to the JOP by the Republic of Korea.

Conflicts of Interest (Recognition Criteria 1-3)

1. *Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A of the Accountability Agent Application for APEC Recognition have been met and submit all applicable written policies and documentation.*
2. *Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A of the Accountability Agent Application for APEC Recognition.*
3. *Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.*

Recommendation

The JOP is satisfied that KISA meets Recognition Criteria 1-3.

Discussion

The JOP has confirmed that as a special legal entity established under the Republic of Korea's laws to perform duties in the public interest, KISA is obligated to perform its certification activities fairly according to the Republic of Korea's laws. Pursuant to the Act on the Management of Public Institutions, KISA is legally obligated to make efforts to reinforce ethical management as a public institution, and MOIS and KCC are obligated to seek investigation or audit of KISA executives if they are suspected of being involved in corruption or believed to have hindered ethical management. As a public institution, KISA is further subject to the Improper Solicitation and Graft Act, which obligates KISA employees to perform their duties fairly and disinterestedly without being affected by private interests, violation of which is punishable by imprisonment or fines.

In addition, the JOP has confirmed that KISA's Code of Conduct requires employees to report potential conflicts of interest to management, who then can reassign the duties of the employee if it is deemed that a conflict would hinder his or her fair performance of duties. Conflicts related to a KISA employee's duties required to be reported include having a familial relationship to an employee or outside director of an organization seeking certification or having worked for an organization in the past two years that is seeking certification. KISA's Code of Conduct prohibits employees from engaging in profit-making activities related to their duties at KISA, including providing paid consulting services related to their duties.

The JOP has further confirmed that KISA has written policies to ensure that a certification

assessor, or the personnel who performs a certification assessment, as well as the CBPR certification committee, or the organization operated by KISA to make decisions on the results of certification assessments, are free from potential or actual conflicts of interest. KISA's Rules on APEC CBPRs certification operation (hereinafter "CBPRs Operating Rules") mandate that certification assessors who participated in consulting for an applicant's CBPR certification or the applicant's employees should be excluded from the certification assessment team. The CBPRs Operating Rules further exclude certification committee members and assessors from being involved in a certification assessment if the member or assessor has a direct stake in the matter, are related to anyone involved in the matter, or in the event that they were involved in the matter before they were appointed. KISA may exclude any committee member or assessor if they cannot guarantee the independence, objectivity, fairness and reliability of a certification.

The JOP has confirmed that KISA will publish the certification standards for applicant and participant organizations, and at least once a year, KISA will submit a certification report to MOIS and KCC, which includes information on new applicants, the number of audits performed, and information on dispute resolution. The JOP has confirmed that as required in criterion 3, KISA will disclose to the JOP conflicts of interest that result in a withdrawal or affiliations that might be on their face be considered a conflict of interest but did not result in a withdrawal.

Program Requirements (Recognition Criterion 4)

Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C of the Accountability Agent Application for APEC Recognition to map its existing intake procedures program requirements.

Recommendation

The JOP is satisfied that KISA meets Recognition Criterion 4.

Discussion

In consultation with the JOP, KISA has used Annex C of the Accountability Agent APEC Recognition Application to map the existing program requirements for its domestic privacy certification system, Personal Information and Information Security Management System (ISMS-P), to the established CBPR program requirements. The JOP has confirmed that KISA will verify that an applicant for CBPR certification meets the ISMS-P program requirements and the CBPR Assessment Criteria set forth in Annex C.

Certification Process (Recognition Criterion 5)

Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (e) of Annex A of the Accountability Agent Application for APEC Recognition have been met.

Recommendation

The JOP is satisfied that KISA meets Recognition Criterion 5.

Discussion

The JOP has confirmed that KISA has a comprehensive process to review whether an applicant organization meets the CBPR program requirements, with the following procedures:

1. The certification applicant submits a self-assessment of whether CBPR program requirements are met, and KISA conducts a preliminary inspection thereof and enters into a contract with the applicant regarding the certification assessment;
2. KISA reviews the applicant's self-assessment, including through written and on-site assessment, and requests remedy or supplementation of program requirements if defects are found;
3. KISA assesses whether defects have been remedied and issues a findings report; and
4. If all requirements are met, KISA issues the certification and provides the relevant details of the certification to be posted on cbprs.org.

On-going Monitoring and Compliance Review Processes (Recognition Criteria 6, 7)

Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d) in the Accountability Agent Application for APEC Recognition.

Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) in the Accountability Agent Application for APEC Recognition.

Recommendation

The JOP is satisfied that KISA meets Recognition Criteria 6, 7.

Discussion

The JOP has confirmed that KISA has internal procedures to ensure the integrity of its certification process and to monitor a participant's compliance with program requirements. Article 25 of the CBPR Operating Rules provides that KISA can assess or audit a participant at any time during the term of a certification. Further, a participant must notify KISA if certified services are changed or if it is deemed too difficult to maintain a certification, and KISA may conduct a verification review after mutual consultation. For a compliance review assessment, KISA may inspect the service environment of the participant on a regular basis, and after consulting with the participant, it may inspect the website online and check technical

vulnerabilities remotely. As described in response to criteria 9 and 10 below, KISA has a mechanism to receive CBPR-related complaints from service users or APEC member economies, providing another avenue for monitoring compliance.

The JOP has confirmed that if there are reasonable grounds to believe that a participant organization is in non-compliance with program requirements, KISA will review a participant organization. If non-compliance is discovered, KISA will prepare a report outlining corrections that need to be made, which must be completed and confirmed in writing to KISA within 90 days. The assessment team leader must check that corrections have been made and submit an auditing report to KISA within 120 days of auditing completion.

Articles 22 and 27 of the CBPRs Operating Rules provides that KISA may suspend a certification assessment or cancel a certification under certain circumstances, such as where an applicant fails to demonstrate compliance with program requirements, fails to take corrective measures within 90 days of being notified of noncompliance, or if a certification was acquired by false or illegal means. If KISA ceases an assessment or cancels a certification, it must notify the applicant or participant the reason for the cancellation.

Re-Certification and Annual Attestation (Recognition Criterion 8)

Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d) in the Accountability Agent Application for APEC Recognition.

Recommendation

The JOP is satisfied that KISA meets Recognition Criterion 8.

Discussion

The JOP has confirmed that pursuant to Article 26 of the CBPRs Operating Procedures, KISA requires an annual re-certification which requires the participant organization to apply for re-certification by 3 months before the expiration of the term of the certification. The JOP has confirmed that KISA may also carry out an assessment if there are significant changes in the scope of certification or if it is deemed necessary, including for changes in certified services, the participant's privacy policy, or certification subjects resulting from mergers and acquisitions. KISA will undertake the assessment process in its entirety as outlined in response to criterion 5 above.

Dispute Resolution Process (Recognition Criteria 9, 10)

Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate.

Applicant Accountability Agent should describe how the dispute resolution process meets the requirements identified in 10 (a) – (h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.

Recommendation

The JOP is satisfied that KISA meets Recognition Criteria 9, 10.

Discussion

The JOP has confirmed that KISA has a mechanism to receive CBPR-related complaints from service users or APEC member economies, and that KISA will require participant organizations to publish on their website the procedures for submitting complaints. Pursuant to Article 29 of the CBPRs Operating Rules, upon receipt of a complaint, KISA will review whether it falls within the scope of CBPR compliance of a participant organization within 10 business days, and if so, will notify the matter to the complainant in writing and investigate the facts. The participant company shall review and respond to the complaint within 30 days or ask for an extension period of up to 30 days. Based on the result of the investigation, KISA may request the certified organization to take corrective measures regarding the inadequacies, and if it fails to do so, KISA may cancel the participant organization's certification. KISA will notify the result of the handling of the complaint to the complainant and the participating organization in writing within 10 business days. KISA will obtain the consent of the individual if it needs to provide personal information to a third party as a part of the complaint handling process. Finally, KISA will make public statistical data on the handling of these complaints and issue case notes in anonymized form on a selection of resolved complaints on an annual basis.

Pursuant to the CBPRs Operating Rules, KISA cooperates with law-enforcement authorities of APEC member economies and accountability agents for handling complaints or cooperation in law enforcement. The JOP has confirmed that KISA will publish on its website the contact points of the relevant government bodies.

Mechanism for Enforcing Program Requirements (Recognition Criteria 11-15)

Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.

Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-

compliance.

Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.

Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].

Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

Recommendation

The JOP is satisfied that KISA meets Recognition Criteria 11-15.

Discussion

The JOP has confirmed that KISA enforces the program requirements through contract with the applicant organization. According to Article 18 of the CBPRs Operating Rules, KISA and a certification applicant will enter into a certification assessment contract, which includes the assessment period, assessors, certificate management and suspension or cancellation of a certification, among other things.

As discussed in response to criterion 7, KISA may notify a participant organization of noncompliance with the program requirements and cancel a certification if a participant organization fails to correct the noncompliance within 90 days pursuant to the CBPRs Operating Rules. The JOP has confirmed that KISA will disclose on its website the company name and other relevant information related to the non-compliance. In addition, KISA can notify MOIS, KCC or other relevant authorities of a violation of program requirements if the violation is serious or intentional pursuant to Article 30 of the CBPRs Operating Rules.

KISA will cooperate with overseas law enforcement authorities of APEC member economies and accountability agents to handle complaints or cooperation in law enforcement pursuant to Article 30 of the CBPRs Operating Rules.

III. CASE NOTES AND STATISTICS

Will the Applicant provide relevant information on case notes and statistics as outlined in Annexes D and E of the Accountability Agent Application for APEC Recognition?

Recommendation

The JOP is satisfied that KISA meets the Case Notes and Statistics requirements as stipulated in Annexes D and E of the *Accountability Agent Application for APEC Recognition*.

Discussion

The Accountability Agent Recognition Criteria 10 (g) & (h) require Accountability Agents to have a process for making publicly available statistics on the types of complaints and the outcomes of such complaints (see Annex E), and a process for releasing, in anonymized form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes (see Annex D). The JOP has confirmed that KISA will make publicly available information on the number of complaints and outcomes of such complaints and release case notes on a selection of important complaints. KISA has agreed to make use of the templates in Annexes D and E of the *Accountability Agent Application for APEC Recognition* to annually send this information to APEC member Economies as a condition of their recognition.

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party agrees to the findings of the Joint Oversight Panel contained herein and attests to the truth of the information provided to the Joint Oversight Panel pursuant to the Application for APEC Recognition.

_____

[Signature of person who has authority to commit party to the agreement]

[Typed name]:

[Date]:

[Typed title]:

[Typed name of organization]:

[Address of organization]:

[Email address]:

[Telephone number]:

APEC recognition is limited to one year from the date of recognition. Each year one month prior to the anniversary of the date of recognition, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.