CROSS-BORDER PRIVACY RULES SYSTEM JOINT OVERSIGHT PANEL

RECOMMENDATON REPORT ON CONTINUED APEC RECOGNITION OF THE KOREA INTERNET AND SECURITY AGENCY (KISA) AS AN ACCOUNTABILITY AGENT FOR THE CBPR SYSTEM

Submitted to: Dr. Ekapong Rimcharone

Chair, Digital Economy Steering Group

26 September, 2023

TABLE OF CONTENTS

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 the Republic of Korea's Ministry of the Interior and Safety 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. On December 14, 2019, KISA received endorsement for APEC recognition as an Accountability Agent for the CBPR System for one year and then was endorsed for an additional two-year term on April 23, 2021.

On March 20, 2023, the Joint Oversight Panel (JOP) received an application from KISA for continued recognition as an APEC Accountability Agent for a subsequent two-year period. After reviewing the application, the JOP found that KISA continues to meet the requirements to serve as an Accountability Agent in the Republic of Korea. KISA's continued recognition as an Accountability Agent will be valid for two years from the date of endorsement.

SCOPE OF CONSULTATION PROCESS

Pursuant to Paragraph 7.2 of the *Charter of the Joint Oversight Panel*, members of the JOP[1] consulted 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* for the CBPR System;
- 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; Makiko Tsuda, Ministry of Economy, Trade and Industry, Japan; and Evelyn Goh, Infocomm Media Development Authority, 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 jurisdiction of the relevant enforcement authority described in Annex A of the Republic of Korea's Notice of Intent to Participate in the CBPR System;

Having verified with the Administrators of the APEC Cross Border Privacy Enforcement Arrangement (CPEA) that Korea's Personal Information Protection Commission (herein 'PIPC') is a participant 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 continued recognition of KISA to certify organizations within the Republic of Korea and under the jurisdiction of the Ministry of Science and ICT (MSICT) and PIPC 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
Infocomm Media Development Authority, Singapore

Makiko Tsuda
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 request for continued 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 for continued recognition, APEC recognition will be limited to two years 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

The JOP has confirmed that KISA is a nonprofit special organization established under the Republic of Korea's 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 MSICT and the PIPC. Pursuant to Article 14 of the Regulation on Delegation and Entrustment of Administrative Authorities, KISA would perform its duties as an Accountability Agent pursuant to the delegated authorities of MSICT and the PIPC. The JOP has confirmed that KISA guides certified companies on compliance with the CBPR system and using the CBPR certification logo when issuing certificates, and KISA conducts monitoring of domestic certified companies' use of the CBPR certification logo by managing a list of certified companies. 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 MSICT and PIPC 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.

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*

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

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 nonprofit special organization 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. Furthermore, KISA operates using government funds and can perform certification activities without any conflict of interest.

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 MSICT and PIPC 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 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 of interest 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, the personnel who performs a certification assessment, and the CBPR certification committee 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 the PIPC, 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 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. **Preparation and Application -** The certification applicant submits an application, and KISA conducts a preliminary check thereof. After that, the applicant pays for the certification fee;
2. **Certification and Application -** KISA conducts written/on-site audits and in the case of non-compliance, KISA requests the applicant remedy the non-compliance. If and when the remedy is completed, KISA issues a findings report;

3. **Deliberation and Issuance –** The certification committee deliberates on the findings report and makes a decision regarding whether to grant certification. Once this decision has been made, KISA issues the certification; and
4. **Compliance Review and Re-Certification -** KISA may request compliance review and/or monitoring of a participant in case of a serious data breach or other case of noncompliance. KISA goes through the same process for the re-certification.

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.

Pursuant to Article 20, 23 and 25 of the Guideline for APEC CBPR Certification (hereinafter 'Guideline'), KISA may request submission of materials, etc. from a certified company if there has been a serious personal information infringement accident, or a complaint is received by the certified companies. Pursuant to Article 23 of the Guideline, KISA may cancel a company's certification when it finds (i) certification is obtained by false or fraudulent means or the organization that has obtained certification fails to comply with it afterwards, (ii) an organizationwho has obtained certification falsely publicizes details of the certification or (iii) an organizationwho has obtained certification does not take necessary measures to handle personal information complaints.

Articles 19 and 23 of the Guideline provides that KISA may suspend the assessment or cancel a certification under certain circumstances, such as where a certification was obtained by false or fraudulent means or fails to comply with the certification requirements. If KISA ceases an assessment or cancels a certification, it must notify the organization that obtained the certification, take back the issued certificate, and disclose the fact.

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 22 of the Guideline, KISA requires a re-certification which requires participants to apply for re-certification by 3 months before the expiration of the term of the certification. Article 20 of the Guideline provides that the certificate is valid for one year. 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 anyone if he/she finds any non-compliance of a certified company, and that KISA will require participant organizations to publish on their website the procedures for submitting complaints.

Pursuant to Article 25 of the Guideline, upon receipt of a complaint, KISA will examine whether the reported matter falls within the APEC CBPR compliance scope of the participant, and if so, may request the organization who has obtained the certification to confirm the fact and make corrections. The participant must take corrective action within 30 days or ask for an extension

period of up to 30 days. Also, KISA offers information on CBPR participants and how to raise questions about CBPR compliance of participants through the CBPR certification webpage. 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 notifies the receipt of the complaint and the result of handling the complaint to the person who filed the complaint and the organization who has obtained certification in writing or electronically. KISA regularly discloses APEC CBPR complaint handling statistics and anonymized casebooks. In the event of receiving complaints, KISA plans to publish related dispute resolution case notes and complaint statistics. KISA has not received any complaints since the CBPR System's launch.

Pursuant to Article 26 of the Guideline, KISA cooperates with foreign law-enforcement authorities of APEC Member economies and APEC CBPR 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 imposing rules on participant organizations which include KISA's authority to suspend or cancel a certification if

certification criteria are not met by an applicant or participant organization.

Pursuant to Article 19 of the Guideline, KISA may suspend an assessment of an applicant organization if the applicant organization delays or interferes with the certification assessment or if the applicant organization fails to meet the program requirements. Pursuant to Article 23 of the Guideline, KISA may cancel a certification when (i) the certification is obtained by false or fraudulent means or the organization that has obtained certification fails to comply with it afterwards, (ii) an organizationwho has obtained certification falsely publicizes details of the certification or (iii) an organizationthat has obtained certification does not take necessary measures to handle personal information complaints. If KISA cancels certification, it must notify the organization that obtained the certification, take back the issued certificate, and disclose the fact.

The JOP has confirmed that KISA may notify a participant organization of its noncompliance with the program requirements and may impose penalties or cancel a certification if a participant organization fails to correct the noncompliance within 30 days pursuant to the CBPRs Operating Rules. Pursuant to Article 24 of the Guideline, an applicant or organization who has obtained certification may file an objection within 15 days when notified by KISA of the deliberation result regarding certification suspension or cancellation. If the certified company has objections to this determination, it can raise an objection within 15 days from the date of notification of the result.

The JOP has confirmed that non-compliance with the CBPR requirements is a violation of Personal Information Protection Act. KISA will promptly notify and discuss serious violations of the CBPR requirements through a constant cooperation system with the PIPC.In addition, KISA has established “Rules for handling complaints and reports” (herein ‘Rules’). Paragraph 1 of Article 4 of the Rules stipulates cases in which received complaints can be transferred to other organizations to enable more sufficient handling of complaints.

Pursuant to Article 26 of the Guideline, KISA has established a system to cooperate with APEC member economies enforcement agencies for handling civil complaints. .

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 of the *Accountability Agent Application for APEC Recognition*), 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 of the *Accountability Agent Application for APEC Recognition*). The JOP has confirmed that in the first year, KISA has not yet certified any companies, and therefore has not submitted any case notes and statistics. The JOP has confirmed KISA began certifying companies in December 2022 and 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. The JOP has confirmed that KISA will make use of the templates in Annexes D and E of the *Accountability Agent Application for APEC Recognition* to 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]:

The first APEC recognition is limited to two years from the date of recognition. One month prior to the second 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: <u>Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law</u>.