APEC CBPR Accountability Agent Renewal Application

1. In regards to APEC CROSS BORDER PRIVACY RULES SYSTEM (hereinafter referred to as 'CBPR'), we, Korea Internet & Security Agency(hereinafter referred to as 'KISA'), are pleased to re-apply for the Accountability Agent.

2. KISA is a public institution established based on the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc(The ICT Network Act), and implements tasks and authority on personal information protection and cyber security which is entrusted or delegated by the each competent authority, the Personal Information Protection Commission(PIPC) and Ministry of Science and ICT(MSIT). According to this, KISA carries out CBPR certification activities as a part of personal information protection tasks, through the business agreement with PIPC. Besides, each competent authority is empowered to conduct or supervise performance of KISA as its delegated or entrusted institution, pursuant to the Regulation on Delegation and Entrustment of Administrative Authorities or the act on the Management of Public Institutions.

<Relavant laws and regulation>

1) The Regulation on Delegation and Entrustment of Administrative Authorities

When the administrative institution delegates a part of its power or authority, or entrust a part of its tasks provided to the related law, to the subsidiary institution or corporate, etc, then the delegated or entrusted institution shall comply the applicable law and carry out tasks faithfully(Article 5). The competent authority is entitled to conduct and supervise the delegated or entrusted institution for the tasks, and suspend or revoke it when illegal or unfair process is found(Article 6, Article 14).

2) Act on the Management of Public Institutions

The public institution such as 'an institution directly established pursuant to other Act with an investment by the government', is obliged to publish the management performance and annual report, etc.(Article 4, Article 11, Article 47, Article 49). The Chief of the competent administrative institution is empowered to supervise performance of the public institution(Article 51).

3) The ICT Network Act

The Government shall establish KISA in order to promote the safe use of the information and communications network, etc and KISA shall perform business affairs including research and development of measures & technology for personal information protection pursuant to the Personal Information Protection Act(PIPA).

4) Personal Information Protection Act(PIPA)

PIPC shall perform business affairs including tasks on establishing and executing policies, cooperating with overseas authorities or international bodies as well as investigating on infringement of data subject right(Article 7-8). Pursuant to PIPA, PIPC entrusts KISA with a power of education on personal information protection, investigation on complaint, etc(Article 68).

3. Also, KISA confirms that the documents necessary for the APEC CBPR Accountability Agent application and additional documents are provided in the form of annexes or appendixes as follows.

1) documents that explain that KISA meets the certification authority approval criteria (Annex A)
2) KISA's detailed certification criteria that conforms to the program requirements of the CBPR (Annex B)
3) The contact information and signature of KISA official in charge of this application (Annex C)
4) KISA's CBPR operating rules (Appendix 1)

4. It will be appreciated if you review above documents and take a necessary step for APEC recognition on our application. For questions, please contact Jaesuk YUN, manager of the Personal Data Cooperation Team(jsyun@kisa.or.kr).

Juyoung KIM
Director of the Personal Data Policy Division at KISA

Annex A

APEC CBPR Accountability Agent Recognition Criteria Checklist

1 Conflict of Interest

Criteria	Operating status of KISA
1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.	◎ Korea Internet & Security Agency(hereinafter KISA) is a special organization established by national policy according to special laws 'the 'Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.(hereinafter Network Act) for the public interest, and as a public agency under the 'Act on the Management of Public Institutions', KISA performs its duties fairly and objectively under the management and supervision of the Ministry of Science and ICT(MSIT), and Personal Information Protection Commission(hereinafter PIPC) etc. Specifically, Paragraph 1 of Article 52 of the Network Act stipulate the purpose of establishing KISA. ◎ KISA is a nonprofit special corporation established for public interests in national policies, and performs duties based on fairness and objectivity under the management and supervision of the competent PEA, the PIPC. Accordingly, unlike associations and organizations which are run based on the membership

Criteria	Operating status of KISA
	fee, or private enterprises whose main purpose is to create profits, KISA runs on government budgets, and the revenues from certification activities are also used for national budget or public purposes. So it can perform certification activities fairly without any interest in certain institutions or business operators. ※ 「**Network Act**」 **Article 52(Korea Internet & Security Agency)** ① The Government shall establish the KISA to upgrade the information and communications network (excluding matters concerning establishment, improvement and management of information and telecommunications network), encourage the safe use thereof, and promote the international cooperation and advancement into the overseas market in relation to broadcasting and communications.
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.	◎ KISA is a public institution that performs public affairs, and is under the supervision and management of the relevant government bodies. According to the 'Improper Solicitation and Graft Act' and other policies of government, KISA is establishing and operating internal regulations such as 「Code of Conduct for Employees」 and regular integrity training sessions for employees` fair performances. ◎ For example, according to Articles 5 and 7 of the 「Code of Conduct for Employees」 of KISA, if the duties employees perform are directly related to themselves, their families, the organizations they worked for in the past, or the

Criteria	Operating status of KISA
	representatives of such organizations, or people who are deemed to have difficulty performing their duties fairly, e.g. people who had financial transactions in excess of a certain amount, KISA must take measures, such as reassignment of duties or manpower. This code of conduct applies to all KISA employees according to Article 3 (Scope of application). ※ **KISA Code of Conduct for Employees Article 3(Scope of application)** This code of conduct will be applied to all employees of KISA. ※ **KISA Code of Conduct for Employees Article 5 (Reporting private interests, etc.)** ① If employees fall under any of the following cases ... they should report it to their superiors or the president of Korea Internet & Security Agency. 1. If employees themselves are persons related to their duties; 2. If the relatives of employees closer than cousins are persons related to their duties; 3. If the corporation and organization for which employees themselves worked in the past 2 years are persons related to their duties; 4. If the corporation and organization in which employees themselves or their families are employees or outside directors are persons related to their duties; and 7. If persons who the president of KISA said are difficult to perform duties fairly are persons related to their duties. ② KISA may request such measures as reassignment of duties for persons related to their duties or persons who have an interest in the duties performed by employees.

Criteria	Operating status of KISA
	④ The president of KISA, who receive the report pursuant to Paragraph 1 or the application pursuant to Paragraphs 2 and 3 may take any of the following measures against such employees if it is deemed to hinder their fair performance of duties. 1. Temporary suspension of participation in duties 2. Designation of a person acting on their behalf or a person who perform duties jointly 3. Reassignment of duties 4. Transfer ※ **KISA Code of Conduct for Employees Article 7 (Prohibition of profit-making activities related to duties)** ① Employees may not do any of the following in relation to the duties of KISA: 1. Privately providing labor, advice or consulting to persons related to their duties and getting paid 2. Representing the counterpart of the agency they belong to or providing advice, consulting or information to the counterpart if they perform duties which involve the agency they belong to in a dispute, or the duties they perform have a direct interest in the agency they belong to ⋮ 5. Behavior related to the duties that the president of KISA deems likely to hinger the fair and disinterested performance of duties ② If the behavior of employees is deemed to fall under any of the following in Paragraph 1, the president of KISA must stop the behavior or order them to

Criteria	Operating status of KISA
	terminate it. ◎ Meanwhile, KISA stipulates the roles and duties of the certification committee and certification assessors through the 「APEC CBPR Operating Rules」 (hereinafter, Rules). Paragraph 4 of Article 12 specifies cases in which certification assessors should be excluded, as those who have participated in the applicants in last 3 years or have experiences in security consulting related work of the applicants in last 3 years, or have any interest with the applicants, are excluded form the certification assessment team. ◎ Also, KISA is preventing various conflicts of interest likely to occur in the process of performing certification and securing independence, fairness, and reliability as a CBPR accountability agent, by stipulating the cases which can exclude, avoid, and evade the certification committee members who have interests with the deliberation agendas, through the Article 9 of the rules. ※ **APEC CBPR Operating Rules Article 9** (Exclusion, avoidance and evasion) ① If certification committee members and assessors on the certification assessment team fall under any of the following in relation to the Certification Applicant, they cannot be involved in or participate in deliberation, voting and certification assessment: 1. In the event that committee members and assessors have a direct stake in the matters,

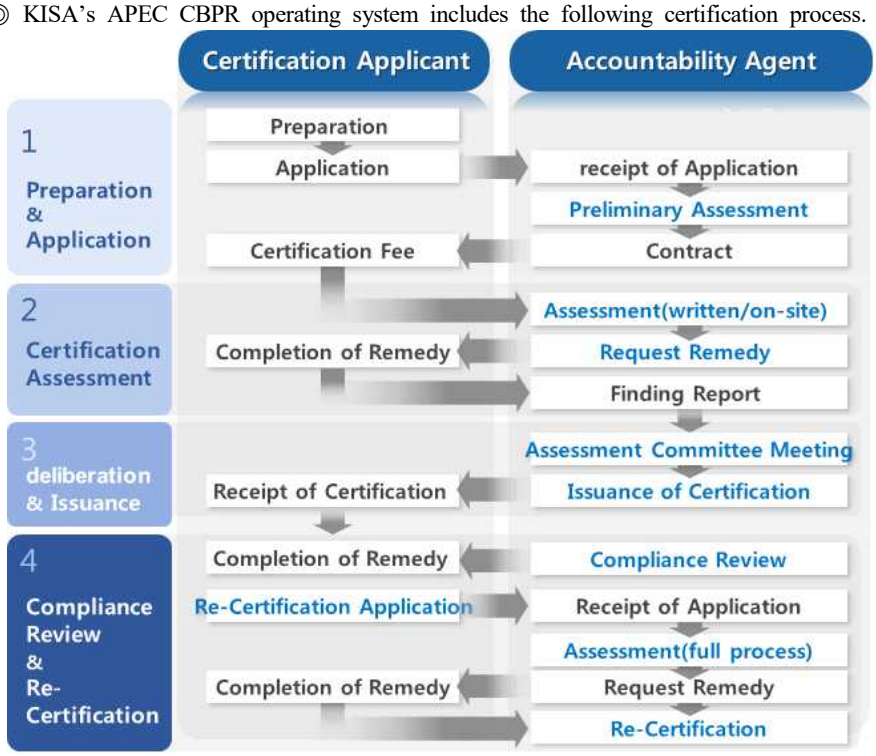
Criteria	Operating status of KISA
	2. In the event that the matters are related to the present or former relatives of committee members and assessors, 3. In the event that committee members and assessors have a direct stake in the matters due to special legal relationships, 4. In the event that committee members and assessors were involved in assessment, investigation or examination of the matters before they were appointed. ※ **APEC CBPR operating rules Article 12 (Composition of certification assessment team)** ④ When organizing the certification assessment team, the following certification assessors should be excluded. 1. Those who belong(work) to the applicant or have an experiences of belonging for the past 3 years 2. Those who have taken related works of applicant such as security consulting, business consignment, etc. 3. Those who have relationship with applicants equivalent to the Paragraph 1 of Article 9
3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.	◎ In accordance with Article 5 of the Rules, the President of KISA may dismiss the committee members when they violate these rules or laws, so that KISA is actually preventing conflicts of interests. ※ **APEC CBPR operating rules Article 5** (Dismiss committee members and appoint supplementary members) ① The President of KISA may dismiss committee members after gathering the opinions of the chairperson, if a member violates laws or these rules.

Criteria	Operating status of KISA
	② A supplementary members may be appointed when any vacancies on committee members occur due to the following reasons. 1. In the case that a committee member is dismissed due to his/her bribery, solicitation from stakeholders, and unfair influences in the process of committee`s activities. 2. In the case that a committee member resigns.

2 Program Requirements

Criteria	Operating status of KISA
4. Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.	◎ KISA is mapping the detailed assessment criteria based on the existing domestic certification system, 'Personal Information & Information Security Management System(ISMS-P) to APEC's 50 CBPR program requirements as shown in <Annex B> to satisfy APEC's criteria.

3 Certification Process

Criteria	Operating status of KISA
5. Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d)* of Annex A have been met.	◎ KISA's APEC CBPR operating system includes the following certification process. 

4 On-going Monitoring and Compliance Review Processes

Criteria	Operating status of KISA
6. 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).	◎ KISA's certification procedures include preliminary check and on-site inspection in addition to the self-assessment, and document review to make sure of the readiness of the applicant and trustable assessment. With the preliminary check, the applicant can be sure that if their information system, procedure is ready for the assessment. Moreover, on-site inspection helps to verify the applicant's self-assessment, making it possible for assessors to access to the internal documents or the information systems, and other relevant equipment which cannot, or should not be disclosed to the outside of company(applicant). ◎ Above all, KISA operates certification committee for the further fairness of assessment. The committee is a independent organization deliberating the findings report of assessment team, and make a decision on issuance of certificate. ◎ To check the participant to adhere to the CBPR, KISA keeps monitoring participants indirectly such as monitoring the relevant media, complaint etc. ※ **APEC CBPR Operating Rules Article 11(Preliminary inspection)** ① KISA may check the applicant`s preparation status for certification assessment through documents review or on-site inspection. ② KISA may request the supplementary measures and postpone the certification assessment if it is impossible to process the certification assessment due to the applicant`s lack of preparation.

	※ **APEC CBPR Operating Rules Article 16** (Certification assessment) ① Certification assessment are conducted in parallel with documents review and on-site inspection. ② Documents review examines the managerial elements by reviewing personal information protection policies and evidence of implementation to the【Appendix 1】. ③ On-site inspection examines the technical elements by interviewing the person in charge, checking related systems and vulnerability in order to confirm the results of the documents review and whether technical and physical safeguard measures have been implemented. ④ KISA completes a defect report【Annex 8】for defects found in the certification assessment, and requests the applicant for supplementary measures. ⑤ When the applicant obtains the Personal Information & Information Security Management System certification (hereinafter referred to as ISMS-P) according to the「Notice on ISMS-P, etc.」and applies for APEC CBPR certification, KISA may assess excluding the overlapped assessment criteria among CBPR assessment criteria in【Appendix 1】in consideration of the scale of personal information processing, business and service characteristics, etc. through consultation with the applicant. ※ **APEC CBPR Operating Rules Article 3** (Composition and roles of the certification committee) ① The President of KISA must install and operate the certification committee to deliberate and make decisions on the following: 1. Results of certification assessment and re-certification assessment

	2. Matters regarding the cancellation of certification or appealing of objections 3. Other matters that the chairperson deems necessary
7. 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) of Annex A.	◎ KISA may request a participant for the relevant details for the compliance review, in case the complaint has received or serious data breach occurred within scope of certification. Following the review, the participant may need to correct for the non-compliance item or KISA may cancel the certificate pursuant to KISA CBPR rules. ※ **APEC CBPR Operating Rules Article 20(Issuance of certification)** ③ KISA may request submission of materials to the certified companies within the scope of certificate when KISA determines it is necessary due to a serious information infringement accident, or a complaint regarding personal information, etc. ※ **APEC CBPR Operating Rules Article 23(Cancellation of certification)** ① KISA may cancel certification after deliberation and voting by the certification committee, when KISA finds the following reasons: 1. In case of obtaining certification by false or fraudulent method 2. In case of the certified company falsely promotes the certified contents 3. When a certified company fails to take measures necessary for handling personal information complaints pursuant to Paragraph 4 of Article 25 ② In the event that certification is canceled pursuant to Paragraph 1, KISA shall recall the issued certification after notifying the company and disclose the

	facts. ※ **APEC CBPR Operating Rules Article 25 (Handling civil complaints related to personal information)** ① Anyone could raise complaint to KISA if he/she founds any non-compliance of certified companies. ② When receiving civil complaints, KISA will review whether they fall within the scope of CBPR compliance of the certified company, and if so, it may request check the fact relevance or corrective measures. ③ If KISA needs to provide personal information to a third party as a part of the process of handling the civil complaints, it must obtain the prior consent of the him/her. ④ Certified company should submit the letter of confirmation of the corrective measures completion to KISA within 30 days from reception of the corrective measure request. ⑤ If certified company needs to extend the period for corrective measures, it shall submit a confirmation letter for period extend and corrective measures plans, and KISA may provide 30 additional days if it is deemed reasonable. ⑥ KISA shall notify the results of corrective measures to complainant and certified company, ⑦ KISA will publish complaint statistics and anonymized case notes regularly.

5 Re-Certification and Annual Attestation

Criteria	Operating status of KISA
8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d)* of Annex A.	◎ CBPR certified organization must apply for re-certification by 3 months before expiration of the term of validity of certification according to Article 22 of the Rules. Re-certification criteria and procedures will comply with the program requirements and procedures described in recognition criterion 5, and if the term of validity of certification expires without applying for re-certification, issued certification will lose effect. ※ **APEC CBPR Operating Rules Article 22(Re-certification assessment)** ① If a certified company want to extend the validity of certification, it shall apply the re-certification 3 months before the expiration date. ② Re-certification assessment is performed in accordance with Chapter 4.

6 Dispute Resolution Process

Criteria	Operating status of KISA
9. 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. 10. 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.	◎ In accordance with Article 25 of the Rules, anyone can raise complaints to KISA when a complaint related to CBPR certification occurs. If the report of the civil petitioner is within the CBPR compliance scope of the certified organization, KISA will notify the reception of the civil complaint to the civil petitioner in wiring or electronic document and check the facts. Based on the result of investigation, KISA may request the certified organization to take corrective measures in regard to inadequacies, and if it fails to do so, it may cancel certification. ※ A**rticle 25 (Handling civil complaints related to personal information)** ① Anyone could raise complaint to KISA if he/she founds any non-compliance of certified companies. ② When receiving civil complaints, KISA will review whether they fall within the scope of CBPR compliance of the certified company, and if so, it may request check the fact relevance or corrective measures. ③ If KISA needs to provide personal information to a third party as a part of the process of handling the civil complaints, it must obtain the prior consent of the him/her. ④ Certified company should submit the letter of confirmation of the corrective measures completion to KISA within 30 days from reception of the corrective measure request.
	⑤ If certified company needs to extend the period for corrective measures, it shall submit a confirmation letter for period extend and corrective measures plans, and KISA may provide 30 additional days if it is deemed reasonable. ⑥ KISA shall notify the results of corrective measures to complainant and certified company, ⑦ KISA will publish complaint statistics and anonymized case notes regularly. ◎ Also, KISA is planning to cooperate with overseas law enforcement authorities or accountability agents, which joined CBPR for the sake of handling civil complaints or cooperation in law enforcement according to Article 28 of the Rules. Therefore, KISA will receive complaints from APEC member economies regarding service of CBPR certified companies, and will publish the complaints case notes to APEC member economies annually. ※ **APEC CBPR Operating Rules Article 26(International Cooperation)** KISA will cooperate with law enforcement authorities or CBPR accountability agents of foreign countries regarding complaints handling and cooperation of legal enforcement.

7 Mechanism for Enforcing Program Requirements

Criteria	Operating status of KISA
11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.	◎ KISA has secured practical enforcement authority for certification applicants and certified companies by establishing regulations in the Rules to suspend certification examination or cancel issued certification. ◎ In accordance with Article 19 of the Rules, KISA stipulates that the certification assessment could be stopped if the applicant`s program requirements are not met. In addition, according to the Article 23 of the Rules, the certification may be canceled if the certified company acquired certification by fraudulent methods or falsely promoted the contents of the certification, or did not take corrective measures for the reported complaint. At this time, KISA retrieves the issued certification and discloses the fact through its CBPR website. ※ **APEC CBPR Operating Rules Article 19(Suspend of assessment)** ① KISA may stop certification assessment in any of the following events: 1. in the event that the certification applicant intentionally delays or interferes with certification assessment, or it is deemed to be difficult to carry on certification assessment due to a reason attributable to the certification applicant 2. in the event that the materials submitted by the certification applicant were reviewed, and it is difficult to say that it is ready for certification
	3. in the event that the supplementary measures pursuant to Article 17 are not taken 4. in the event that it is deemed to be impossible to carry on certification assessment due to natural disasters and changes in the business environment ※ **APEC CBPR Operating Rules Article 23(Cancellation of certification)** ① KISA may cancel certification after deliberation and voting by the certification committee, when KISA finds the following reasons: 1. In case of obtaining certification by false or fraudulent method 2. In case of the certified company falsely promotes the certified contents 3. When a certified company fails to take measures necessary for handling personal information complaints pursuant to Paragraph 4 of Article 25 ② In the event that certification is canceled pursuant to Paragraph 1, KISA shall recall the issued certification after notifying the company and disclose the facts. ◎ The regulations on the suspension of assessment and cancellation of certification are applied through the entire certification application and maintenance process between KISA and the company, and have the same effect as the contract between the two parties. Therefore, KISA is securing the executive authority based on the contractual effect of the certification body.
12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of	◎ As discussed in the accountability agent checklist 10 and 11, KISA notify non-compliance of the certified company in accordance with Article 20 and 25, and may impose penalties regarding it.

non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance. 13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e)* of Annex A.	◎ If it is confirmed that the certified company does not comply with the CBPR requirements, KISA may request corrective measures on it, and if those measures are not implemented within the specified time limit, the certification may be canceled according to the deliberation and voting of the certification committee. 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. ※ **APEC CBPR Operating Rules Article 24 (Appeal objection)** ① A certified company may raise an appeal within 15 days when it is notified the result of deliberation on cancellation of certification. At this time, the company shall submit the【Annex 7】to KISA. ② If the objection pursuant to Paragraph 1 is considered reasonable, KISA may request re-consideration to the certification committee. ③ KISA shall notify the applicant or certified company the result of handling the objection by written documents.
14. 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].	◎ The Personal Information Protection Commission(hereinafter 'PIPC') is an enforcement authority of Personal Information Protection Act(hereinafter 'PIPA') which joined CBPR, and KISA is a public organization that supports affairs such as research on personal information protection policies and technology dissemination of the PIPC(refer to the checklist 1). In many cases, non-compliance with the CBPR requirements is a violation of PIPA, and KISA promptly notify and discuss about serious violations through a constant cooperation system with PIPC. ◎ In addition, KISA has established 「Rules for handling complaints and reports」 in order to determined details necessary for handling received complaints, and Paragraph 1 of Article 4 of thess rules stipulate cases in which received complaints can be transferred to other organizations so that more sufficient handling on complaints is possible. ※ **Rules for handling complaints and reports Article 4(Principles of handling)** ① In principle, KISA shall handle complaints received by itself. However, if it falls under any of the following, it may be transferred to other organizations. 1. When it is determined that the content of received complaint is not under the responsibility of KISA 2. When it is deemed appropriate to be handled by related other organizations 3. When it is determined that transferring to other organization is more helpful to the complainant
15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.	◎ As discussed in the accountability agent checklist 9, KISA is establishing cooperative system for handling the civil complaint with enforcement authorities of APEC member economies and CBPR accountability agents. In addition, through a cooperative system with PIPC which is a member organization of APEC CPEA, KISA is maintaining the responding system for CBPR related complaints within APEC.

Annex B

KISA has developed our CBPRs assessment criteria making use of assessment checklist of our domestic Privacy Certification System, 'Personal Information & Information Security Management System(ISMS-P)', for demonstrating that it meets the baseline of APEC CBPRs Program Requirements.

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS MAP

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant organization's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

※ The number(*) came from the numbers on the ISMS-P checklists

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	Program Requirement of KISA
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible.	3.5.1 You must establish the personal information processing policy, including all necessary matters like the purpose of processing personal information, and disclose it and continuously update it in such a way that the data subject (user) can always check it easily.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria** (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	• Applies to all personal information; whether collected online or offline. States an effective date of Privacy Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria** (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria** (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the	

Question (***to be answered by the Applicant Organization***)	**Assessment Criteria** (***to be verified by the Accountability Agent***)	Program Requirement of KISA
	Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a **functional** e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria** (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	verify whether the applicable qualification is justified.	
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.f) Does this privacy statement provide information	Where the Applicant answers **YES**, the Accountability Agent must verify that the	

Question (***to be answered by the Applicant Organization***)	**Assessment Criteria** (***to be verified by the Accountability Agent***)	Program Requirement of KISA
regarding whether and how an individual can access and correct their personal information?	Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification,	

Question (***to be answered by the Applicant Organization***)	**Assessment Criteria** (***to be verified by the Accountability Agent***)	Program Requirement of KISA
	the Accountability Agent must verify whether the applicable qualification is justified.	
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	Program Requirement of KISA
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives.

Question (***to be answered by the Applicant Organization***)	**Assessment Criteria** (***to be verified by the Accountability Agent***)	Program Requirement of KISA
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. 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.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	1.2.2 You must analyze the current status of information service and personal information processing with regard to all areas of the management system, identify and document the business procedure and flow, periodically review them and keep them up-to-date.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • 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. Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes	3.1.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided. 3.1.5 If you collect or receive personal information from someone other than the data subject (user), you must collect and use only the minimum personal information necessary for business, and if it is based on laws, or the data subject (user) requests it, you must notify the source of the personal information, purpose of processing personal information, and the right to demand suspension of processing.

Question (***to be answered by the Applicant Organization***)	**Assessment Criteria** (***to be verified by the Accountability Agent***)	**Program Requirement of KISA**
	Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives.

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This 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 applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information	Where the Applicant answers YES, the Accountability Agent must verify the existence of written policies and procedures to ensure that all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes.	3.2.5 You must use or provide personal information only for the purposes to which the data subject (user) consented when it was collected or to the extent based on laws, and if you want to use or provide it otherwise, you must obtain additional consent from the data subject (user), or check if it is legal according to related laws, and establish and implement appropriate safeguard measures.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below.	
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual?	Where the Applicant answers NO to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail	3.2.5 You must use or provide personal information only for the purposes to which the data subject (user) consented when it was collected or to the extent based on laws, and if you want to use or provide it otherwise, you must obtain additional consent from the data subject (user), or check if it is legal according to related laws, and establish and implement appropriate safeguard measures.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
9.b) Compelled by applicable laws?	• Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify). Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant answers YES in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred;	3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.
11. Do you transfer personal information to personal information processors? If YES, describe.		3.3.2 If personal information processing is outsourced to a third party, you must inform the data subject (user) of related information, e.g. the details of outsourced tasks and the third party, and obtain consent if necessary.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.	2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Usingtheabove,theAccountabilityAgentmustverifythattheApplicant'sdisclosuresortransfersofallpersonalinformationislimitedtothepurpose(s)ofcollection,orcompatibleorrelatedpurposes.	3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.
		3.3.2 If personal information processing is outsourced to a third party, you must inform the data subject (user) of related information, e.g. the details of outsourced tasks and the third party, and obtain consent if necessary.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?	Where applicant answers NO to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes.	3.2.5 You must use or provide personal information only for the purposes to which the data subject (user) consented when it was collected or to the extent based on laws, and if you want to use or provide it otherwise, you must obtain additional consent from the data subject (user), or check if it

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	Where the Applicant answers YES to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers YES to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the	is legal according to related laws, and establish and implement appropriate safeguard measures.

Question (*to be answered by the Applicant Organization*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers YES to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers NO to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or	3.1.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	• Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated Where the Applicant answers NO, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be	3.1.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify)	3.1.1 Personal information should be collected legally and legitimately on a minimal scale for the provision of services, and when collecting personal information other than essential information, it should be classified as optional items and should not refuse to provide the service because the relevant information is not provided.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.]	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers NO, or when	(Addition) When you obtain consent, the data subject (user) must be notified so that he/she can clearly recognize and confirm the contents to be consented.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
their personal information, are they displayed or provided in a clear and conspicuous manner?	the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers NO, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow	(Addition) When you obtain consent, the data subject (user) must be notified so that he/she can clearly recognize and confirm the contents to be consented.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	(Addition) When you obtain consent, the data subject (user) must be notified so that he/she can clearly recognize and confirm the contents to be consented.
		(Addition) Methods for requesting withdrawal of consent, access to and provision of personal information, correction of errors, etc. should be provided in a way that is easier than collecting methods.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to verify and ensure	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures/steps to verify and	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	or other service providers acting on the Applicant's behalf. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed?	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
If YES, describe.	Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	1.1.5 You must establish and prepare data protection and personal information protection policies and implementation documents that clearly present the data protection and personal information protection policies and directions of the organization. Also, you must have the policies and implementation documents approved by the management including the CEO, and deliver them to employees and related persons in a form that they can easily understand.
27. Describe the physical, technical and administrative safeguards you have	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal	1.3.1 You must effectively implement the selected safeguard measures according to the implementation plan, and the management boards must check the

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (eg password protections) • Encryption • Boundary protection (eg firewalls, intrusion detection) • Audit logging • Monitoring (eg external and internal audits, vulnerability scans) • Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal	accuracy and effectiveness of the implementation results.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle	
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that	1.2.3 You must collect information on threats by type through analysis of the environment in and outside of the organization, select the right risk assessment method for the organization, assess the risk in all areas of the management system at least once a year, and have acceptable risks approved by the management.
		1.2.4 You must select safeguard measures appropriate for the organization to handle the risks identified according to the result of risk assessment, establish the implementation plan, including priorities and schedules of safeguard measures, persons in

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	charge and budgets, and have it approved by the management.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through	2.2.4 You must establish and operate annual awareness enhancement plans and education and training plans so that employees and related outsiders can understand the management systems and policies of the organization, and secure expertise for each job.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	
30. 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:	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the	1.3.1 You must effectively implement the selected safeguard measures according to the implementation plan, and the management boards must check the accuracy and effectiveness of the implementation results.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
30.a) Employee training and management or other safeguards?	existence of safeguards on each category is required for compliance with this principle.	2.2 Personal security
		2.3 Outsider security
30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?		2.9 System and service operations management
		2.10 System and service security management
30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?		2.11 Incident prevention and response
30.d) Physical security?		2.4 Physical security
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information.	3.4.1 You must establish internal policies related to the retention period and destruction of personal information, and if it is time to destroy the personal

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	information, e.g. the personal information retention period expires and the processing purpose is accomplished, you must immediately destroy it in a way that can guarantee the safety and completeness' of destruction.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle	2.9.5 To guarantee the normal use of the information system and prevent user misuse and abuse (unauthorized connections, excessive access, etc.), you must establish the log review standards for access and use, periodically inspect them, and take timely measures in case there are problems.
		2.10.1 You must establish and implement the operating procedures, e.g. designating administrators for security system types, updating the policies, changing the rule sets and monitoring events, and manage the status of policy application to each security system.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
		2.11.1 To prevent infringements and personal information leakage, and quickly and effectively respond to incidents, you must establish systems and procedures for detecting, responding to, analyzing and sharing internal and external intrusion attempts, and build a system for cooperating with related external agencies and experts.
		2.11.3 To quickly detect and respond to internal and external infringement attempts, personal information leakage attempts and illegal behavior, you must collect and analyze such network and data flow, and take timely measures according to the results of monitoring and inspection.
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	2.11.4 To make employees and stakeholders familiarize themselves with the procedure for responding to infringements and personal information leakage incidents, you must conduct simulation training based on scenarios at least once a year,

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
		and reflect the result of the training and improve the response system.
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	1.2.3 You must collect information on threats for each type through internal and external environment anaysis of the organization, and evaluate risks for all areas of the management system at least once a year by selecting appropriate risk assessment methods, and manage acceptable risks approved by the administrative members.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access,	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against	2.3.2 If you are using external services or outsourcing business to outsiders, you must identify information protection and personal information protection requirements, and specify related contents in the contract or agreement.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking safeguard measures according to the information protection and personal information protection requirements, specified in the contract, agreement and internal policies.

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this are directed towards ensuring that individuals are able to access and correct their information. This includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
36. Upon request, do you provide confirmation of whether or not you hold personal	Where the Applicant answers **YES**, the Accountability Agent must verify that the	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
information about the requesting individual? Describe below.	Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the	subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?	appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that	individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?		

ACCOUNTABILITY

Assessment Purpose - *The questions in this are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable,	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	1.4.1 You must periodically check the legal requirements, related to information protection and personal information protection, that the organization must comply with.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations ____ • Compliance with self-regulatory applicant code and/or rules ____ Other (describe) ____		
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the	1.1.2 The CEO must appoint executives who can allocate resources like budgets and manpower, as the chief information security officer who supervises information protection, and a chief privacy officer who supervises information protection, and the chief privacy officer who supervises personal information

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	protection.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g.	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.
42. Do you have procedures in place to ensure individuals	Where the Applicant answers **YES,** the Accountability Agent must verify that the	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
receive a timely response to their complaints?	Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
		must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	2.2.4 You must establish and operate annual awareness enhancement plans and education and training plans so that employees and related outsiders can understand the management systems and policies of the organization, and secure expertise for each job.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers **YES, the** Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	(Addition) Procedures for carrying out government affairs must be prepared and implemented according to it.
		(Addition) In the case of providing personal information of a data subject (user) to a third party, it must be based on laws or regulations, or must notify all related matters and obtain consent.
		(Addition) Personal information handlers and executives and employees in the organization should take separate training necessary to enhance professionalism according to job characteristics in relation to personal information protection.
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described.	2.3.1 If you are outsourcing part of your business (personal information handling, information protection, information system operation or development, etc.) to the outside, or using external

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-regulatory applicant code and/or rules _____ Other (describe) _____	Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	facilities or services (Internet Data Center, cloud service, application service, etc.), you must identify the status and the legal requirements and risks from external organizations and services, and establish appropriate protective measures.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement?_____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement?_____ • Follow instructions provided by you relating	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	2.3.2 If you are using external services or outsourcing business to outsiders, you must identify information protection and personal information protection requirements, and specify related contents in the contract or agreement.
		2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking protective measures according to the information protection and personal information protection requirements, specified in the contract, agreement and internal policies.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
to the manner in which your personal information must be handled?_____ • Impose restrictions on subcontracting unless with your consent? _____ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ • Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? Other (describe) _____		

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below	The Accountability Agent must verify the existence of such self-assessments.	2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking protective measures according to the information protection and personal information protection requirements, specified in the contract, agreement and internal policies.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking protective measures according to the information protection and personal information protection requirements, specified in the contract, agreement and internal policies.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	(Addition) When personal information is transfered to a third party for purposes other than the purpose of collection, the recipient should be asked to limit the purpose and method of use, or to take necessary measures to ensure safety. (Addition) When the processor re-consigns personal information processing to a third party, it re-consigns only when the controller's consent is obtained, and the processor should manage and supervise the re-consignee to implement the same level of technical and administrative protection measures that the controller requests to the processor.

Annex C

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party attests to the truth of the answers given.

 Juyoung KIM April 07, 2021

[title] **Director**

[name of organization] **Korea Internet & Security Agency**

[Address of organization] **9, Jinheung-gil, Naju-si, Jeollanam-do, Korea, 58324**

[Email address] **kjy@kisa.or.kr**

[Telephone number] **82-61-820-1810**

The first APEC recognition for an Accountability Agent is limited to one year from the date of recognition. Recognition for the same Accountability Agent will be for two years thereafter. One month prior to the end of the recognition period, 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.

APEC CBPR Operating Rules

Enacted 2020.12.

Chapter 1 General Provisions

Article 1 (Purpose) The purpose of these rules is to stipulate matters necessary for fair execution of APEC CBPR certification tasks assigned as the duties of the Personal Information Protection Division in accordance with the Regulations on the organization of KISA.

Article 2 (Definitions of terms) The terms used in these regulations are defined as follows:

1. “CBPR certification” refers to the official recognition that the Certification Applicant’s measures and activities to protect personal information conform to the CBPR certification criteria in 【Appendix 1】.
2. "Certification assessment" refers to confirmation of whether the activities related to personal information protection, which are established and conducted by the Certification Applicant, conform to the CBPR certification criteria in 【Appendix 1】 using such methods as preliminary, written and on-site review, etc.
3. "CBPR certification committee (hereinafter referred to as the ‘certification committee’)" refers to the organization installed and operated by the head of the KISA to deliberate and make decisions on the results of certification assessment, which consists of the chairperson and committee members.
4. "Certification assessor" refers to the person, who are recognized to be qualified for perform the certification assessment from KISA.
5. “Committee member” refers to the person who consist of the certification committee.
6. “Supplementary member” refers to the committee member who are designated for supplement the vacancy at the committee.
7. "Applicant" refers to the corporations and institutions which applied to KISA for CBPR certification.
8. “Preliminary assessment” refers to the review process conducted before certification assessment to check whether the Certification Applicant’s self-assessment result, which describes the Applicant’s personal information protection system and its operation in accordance with the certification criteria, and the related evidential materials are appropriate.
9. “Re-certification assessment” refers to the certification assessment conducted when re-certification is requested as the term of validity expired.
10. “Defect” refers to the matter which are not met for the requirements of CBPR assessment criteria in 【Appendix 1】.

Chapter 2 Organization and operation of the certification committee

Article 3 (Composition and roles of the certification committee) ① The President of KISA must install and operate the certification committee to deliberate and make decisions on the following:

1. Results of certification assessment or re-certification assessment
2. Matters regarding the cancellation of certification or objection of an Applicant
3. Other matters that the chairperson deems necessary

② The certification committee consist of around 10 committee members who have knowledge and experience in personal information protection, and the chairperson will be elected by the committee from among its members.

③ The chairperson will oversee the certification committee and represent the committee.

④ The President of KISA may dismiss committee members if they violated any

laws or these regulations.

⑤ Certification committee has secretary, and the head of a team which organizes the CBPR certification is appointed as the secretary.

Article 4 (Duties of committee members) Committee members shall comply with the following duties.

1. Committee members shall deliberate the results of certification assessment and the issuance of certification fairly and objectively.

2. Committee members maintain dignity and faithful performance.

3. Committee members shall deny commercial, financial, and other types of pressures regarding deliberation.

4. Committee members shall submit 【Annex 15】oath of ethics and 【Annex 16】 oath of confidentiality to KISA regarding the above terms of compliance.

Article 5 (Dismiss committee members and appoint supplementary members) ① The President of KISA may dismiss committee members after gathering the opinions of the chairperson, if a member violates laws or these rules.

② A supplementary members may be appointed when any vacancies on committee members occur due to the following reasons.

1. In the case that a committee member is dismissed due to his/her bribery, solicitation from, or unfair influences to, stakeholders, in the process of committee`s activities.

2. In the case that a committee member resigns.

Article 6 (Term of committee members) ① Term of committee members is 3 years and they may serve consecutive terms through reorganization of committee.

② Term of supplementary members is the remaining period of their predecessor.

Article 7 (Hosting and operation committee meetings) ① Certification committee meetings will be convened when the deliberation of assessment results is required or it is deemed necessary to host a committee meeting.

② Committee may deliberate and make decisions though online or written documentations when it is impossible to host the meeting due to any urgent reasons or the agenda for deliberation is deemed minor.

③ The chairperson of committee shall submit the results of deliberation of Paragraph 1 of Article 3 to the President of KISA.

④ Other detailed matters regarding operation of Committee is determined by the President of KISA through decisions of committee.

Article 8 (Quorum of committee`s hosting and decision makings) ① Certification committee meeting is held only the majority of committee members attend including the chairperson. However, if the chairperson is unable to perform his/her duties due to unavoidable reasons, a member appointed in advance shall act as the chairperson.

② The agenda for voting will be passed with the approval of at least two-thirds of the members consent.

Article 9 (Exclusion, avoidance and evasion) ① If certification committee members and assessors on the certification assessment team fall under any of the following in relation to the Certification Applicant, they cannot be involved in or participate in deliberation, voting and certification assessment:

1. In the event that committee members and assessors have a direct stake in the matters,

2. In the event that the matters are related to the present or former relatives of committee members and assessors,

3. In the event that committee members and assessors have a direct stake in the matters due to special legal relationships,

4. In the event that committee members and assessors were involved in assessment,

investigation or examination of the matters before they were appointed.

② If there are circumstances in which it is difficult for the parties to the relevant agenda to expect an impartial deliberation and decision makings from the committee, the parties to the agenda may apply avoidance to the committee, and the committee decides it by resolution. In this case, the member who is the subject for the avoidance cannot participate in the deliberation.

③ If the committee member falls under the reason for the exclusion pursuant to each subparagraph of the Paragraph 1, the member may avoid deliberation and decisions on the agenda by himself.

Chapter 3 Application of certification

Article 10 (Preparation by the Certification Applicant in advance) ① The Certification Applicant shall submit the following to KISA before certification assessment:

1. 【Annex 2】 APEC CBPR application
2. 【Annex 3】Applicant’s operation state on personal information
3. Applicant`s self-assessment results for the CBPR certification criteria in 【Appendix 1】.
4. Business license
5. Documents that can prove if the applicant is subject to adjustment of the certification fee

② KISA can request supplement if the submitted documents are insufficient or lacked.

③ Applicant shall supplement the application documents within 10 days from request, and it is deemed the application is abandoned if it is not carried on before the deadline.

Article 11 (Preliminary assessment) ① KISA may check the applicant`s preparation status for certification assessment through documents review or on-site inspection.

② KISA may request the supplementary measures and postpone the certification assessment if it is impossible to process the certification assessment due to the applicant`s lack of preparation.

Chapter 4 Certification assessment

Article 12 (Composition of assessment team) ① KISA shall form assessment team when the assessment schedule is confirmed.

② Assessment team consists of persons who are recognized as capable of carrying on the certification assessment, and KISA establish detailed principles on composition and operation of assessment team.

③ The head of assessment team shall be designated among an assessor who are belong to KISA.

④ When organizing the certification assessment team, the following certification assessors should be excluded.

1. Those who belong(work) to the applicant or have an experiences of belonging for the past 3 years
2. Those who have taken related works of applicant such as security consulting, business outsourcing, etc.
3. Those who have relationship with applicants equivalent to the Paragraph 1 of Article 9

Article 13 (Roles of assessment team) ① The head of assessment team shall perform duties of following:

1. Establish assessment plan, execute whole assessment, and report assessment results

2. Distribute of duties to each assessor
3. Check supplementary measures on defects found in assessment
4. Evaluate of assessors on their assessment activities
5. Prepare assessment results report
6. Report assessment result to the certification committee

② Assessors shall carry on following duties

1. Establish assessment plan and perform assessment on assigned duties
2. Write and submit defect report
3. Support to and cooperate with the head of assessment team.

Article 14 (Duties of assessors) Assessors shall comply with the following duties.

1. Assessors shall perform objective and fair assessment.
2. Assessors maintain dignity and faithful performance.
3. Assessors shall deny commercial, financial, and other types of pressures regarding assessment.
4. Assessors shall submit 【Annex 17】oath of ethics and 【Annex 18】 oath of confidentiality to KISA regarding the above terms of compliance.

Article 15 (Expense for assessment) ① KISA shall pay advisory fee and travel expenses according to the 【Appendix 2】.

② In the case that assessors perform their duties domestically and aborad, KISA pay the fixed cost for transportation, meals, and accommodation, in accordance with KISA 「Rules for Business Trip」.

③ KISA may charge costs necessary for the certification assessment to the applicant.

Article 16 (Certification assessment) ① Certification assessment are conducted in parallel with documents review and on-site inspection.

② Documents review examines the administrative elements by reviewing personal information protection policies and evidential materials, whether it is appropriate com pared to the【Appendix 1】CBPR certification criteria.

③ On-site inspection examines the technical, physical elements by interviewing the person in charge, checking related systems and vulnerability in order to confirm the results of the documents review.

④ KISA completes a defect report 【Annex 8】 for defects found in the certification assessment, and requests the applicant for supplementary measures.

⑤ When the applicant obtains the Personal Information & Information Security Management System certification (hereinafter referred to as ISMS-P) according to the 「Notice on ISMS-P, etc.」 and applies for APEC CBPR certification, KISA may assess excluding the overlapped assessment criteria among CBPR assessment criteria in 【Appendix 1】CBPR certification criteria, in consideration of the scale of personal information processing, business and service characteristics, etc. through consultation with the applicant.

Article 17 (Supplementary measure) ① The applicant shall perform the supplementary measures within 40 days from the date of receipt of the request for it, and should submit the written statement of the supplementary measures to KISA along with the completion of it.

② In the case of the supplementary measures are not completed within 40 days, applicant shall write and submit 【Annex 12】 summary report for supplementary measures on the remained defects along with request letter for the extension to KISA. If the head of assessment team determines the reason for extend is reasonable, the head may provide up to 60 additional days for supplementary measures.

③ The head of assessment team may visit the site and check the results if it is determined that on-site confirmation is necessary for the details of the supplementary measures submitted by the applicant.

④ Completion of the supplementary measures referred to in Paragraph 2 refers to the submission of the report on confirmation of the supplementary measures 【Annex 1

3】including the signature of the applicant`s data protection officer and the head of the assessment team.

Article 18 (Results reporting) The head of assessment team shall confirm status of supplementary measures, and submit a final report of the assessment to KISA within 120 days.

Article 19(Suspend of assessment) ① KISA may suspend certification assessment in any of the following events:

1. in the event that the certification applicant intentionally delays or interferes with certification assessment, or it is deemed to be difficult to carry on certification assessment due to a reason attributable to the certification applicant
2. in the event that the materials submitted by the certification applicant were reviewed, and it is difficult to say that it is ready for certification
3. in the event that the supplementary measures pursuant to Article 17 are not taken
4. in the event that it is deemed to be impossible to carry on certification assessment due to natural disasters and changes in the business environment

② If certification assessment is suspended, the applicant must fill out and submit the 【Annex 10】 Letter of confirmation for suspension of assessment to KISA.

③ If the reason for the cessation of certification assessment in Paragraph 1 is removed, or according to the result of the objection raised pursuant to Article 24, KISA may resume or terminate certification assessment.

Chapter 6 Issuance and management of certification

Article 20 (Issuance of certification) ① When the President of KISA has been informed the deliberation results of the certification committee, he/she should notify it to applicant, and issue 【Annex 4】 the certificate if it is determined to appropriate to the 【Appendix 1】 CBPR certification criteria..

② The valid date of certification on Paragraph 1 is 1 year.

③ KISA may request submission of relevant materials to the certified companies within the scope of certificate when KISA determines it is necessary due to a serious information infringement accident, or a complaint regarding personal information on the Applicant, etc.

Article 21 (Management and re-issuance of certification) ① KISA shall manage the details such as certification number, issued date, valid date, etc of issued certifications.

② If a certified company needs re-issuance of certification due to loss of certification and etc, it shall submit 【Annex 5】 application for re-issuance of certification to KISA.

③ If a certified company needs to correct stated matters on certification such as name of business, representative of business and etc, it shall submit 【Annex 6】 application for correction of certification to KISA.

④ KISA shall submit 【Annex 1】 annual report including number of assessment performed, number of complaints processed, and etc, to Personal Information Protection Commission more than 1 time yearly.

Chapter 8 Follow-up management of certificates

Article 22 (Re-certification assessment) ① If a certified company want to extend the validity of certification, it shall apply the re-certification 3 months before the expiration date.

② Re-certification assessment is performed in accordance with Chapter 4.

Article 23 (Cancellation of certification) ① KISA may cancel certification after deliberation and voting by the certification committee, when KISA finds the

following reasons:

1. In case of obtaining certification by false or fraudulent method or failing to comply with it after obtaining certification
2. In case of the certified company falsely publicizes the certified contents
3. When a certified company fails to take measures necessary for handling personal information complaints pursuant to Paragraph 4 of Article 25

② In the event that certification is canceled pursuant to Paragraph 1, KISA shall recall the issued certification after notifying the company and disclose the facts.

Article 24 (Appeal objection) ① A certified company may raise an appeal within 15 days when it is notified the result of deliberation on cancellation of certification. At this time, the company shall submit the 【Annex 7】 to KISA.

② If the objection pursuant to Paragraph 1 is considered reasonable, KISA may request re-consideration to the certification committee.

③ KISA shall notify the applicant or certified company the result of handling the objection by written documents.

Article 25 (Handling complaints related to personal information) ① Anyone could raise complaint to KISA if he/she founds any non-compliance of certified companies.

② When receiving complaints, KISA will review whether they fall within the scope of CBPR compliance of the certified company, and if so, it may request check the fact relevance or corrective measures.

③ If KISA needs to provide personal information to a third party as a part of the process of handling the civil complaints, it must obtain the prior consent of the him/her.

④ Certified company should submit the letter of confirmation of the corrective measures completion to KISA within 30 days from receipt of the corrective measure request.

⑤ If certified company needs to extend the period for corrective measures, it shall submit a confirmation letter for period extend and corrective measures plans, and KISA may provide 30 additional days if it is deemed reasonable.

⑥ KISA shall notify the results of corrective measures to complainant and certified company,

⑦ KISA will publish complaint statistics and anonymized case notes regularly.

Article 26 (International cooperation) KISA will cooperate with law enforcement authorities or CBPR accountability agents of foreign countries regarding complaints handling and cooperation of legal enforcement.

Article 27 (Confidentiality) Those who work in certification assessment such as KISA, certification committee members, assessors, etc shall not disclose or use information acquired during their works without due authority or permitted authority.

Annex A

KOREAN DOMESTIC LAWS AND REGULATIONS APPLICABLE TO ACCOUNTABILITY AGENT ACTIVITIES

APEC-recognized CBPR Accountability Agents operating in Korea may be subject to the following domestic laws in respect of their certification activities, as follows:

If an APEC-recognized Accountability Agent is a "special corporation" (a generic term for corporations established in accordance with a special law for public interests pursuant to national policies), it shall be managed and supervised by the competent authorities in accordance with the law on the establishment of the corporation. Korea Internet & Security Agency (KISA), which is in charge of operating the domestic personal data protection certification system, was established in accordance with Article 52 (Korea Internet & Security Agency) of the *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.*, Article 68 (Delegation and Entrustment of Authority) of the *Personal Data Protection Act*, and Article 62 (Delegation of Authority) of the *Enforcement Decree of the Personal Data Protection Act*. As such, the certification-related activities of KISA are overseen by the Korea Communications Commission or the Ministry of the Interior.

In addition, if an APEC-recognized Accountability Agent is a private enterprise, such as a manufacturing or service enterprise to whom this law applies (enterprise under Article 2 of the *Monopoly Regulation and Fair Trade Act*), it shall be regulated by the *Act on Fair Labeling and Advertising,* which prohibits unfair labeling and advertising of goods or services that would likely cheat or mislead consumers, such as false or exaggerated labeling or advertising, and fraudulent labeling or advertising, as stipulated in Article 3 (Prohibition, etc. of Unfair Labeling or Advertising) of the *Act on Fair Labeling and Advertising*. Furthermore, the acts that will induce other enterprises to address such labeling or advertising shall be also regulated. Should an APEC-recognized Accountability Agent violate this Article, the Fair Trade Commission, as the competent authority, shall order suspension of the violation, publication of the fact that a corrective order has been issued to the relevant business entities, and correction of the advertising in accordance with Article 7 (Corrective Measures) of the *Act*.

Finally, if an APEC-recognized Accountability Agent is a non-profit corporation (an association or a foundation established for non-profit purpose), it shall be regulated by the relevant oversight administrative agency authorized to inspect and supervise the business of the corporation in accordance with Article 37 (Inspection and Supervision over Business of Juristic Person) of the *Civil Act*. If an ultra-vires act of an APEC-recognized Accountability Agent causes any damage to other persons, it shall be liable for the damages caused thereby in accordance with Article 35 (Capacity of Juristic Person to Assume Responsibility for Unlawful Act) of the *Civil Act*, and the relevant oversight authorities may cancel the permission of the incorporation of the APEC-recognized Accountability Agent in accordance with Article 38 (Cancellation of Permission for Incorporation of Juristic Person).

Annex B

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP

As outlined in the Charter of the APEC Cross Border Privacy Rules (CBPR) System's Joint Oversight Panel (JOP), an APEC Member Economy is considered a Participant in the CBPR System after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met:

(i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA);

(ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter of the JOP;

(iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the JOP, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and

(iv) The JOP submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied.

The purpose of Annex B is to assist Economies and the JOP in fulfilling the requirements of items (iii) and (iv):

- *This document provides the baseline program requirements of the APEC Cross Border Privacy Rules (CBPR) System in order to guide the Economy's explanation of how each requirement may be enforced in that Economy; and*
- *The information provided by the Economy will form the basis of the JOP's report.*

Column 1 lists the questions in the intake questionnaire to be answered by an applicant organization when seeking CBPR certification. Column 2 lists the assessment criteria to be used by an APEC-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Economy's ECSG delegation or appropriate governmental representative when explaining the enforceability of an applicant organization's answers in Column 1. An economy's relevant privacy enforcement authorities should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements. Additional documentation to assist in these explanations may be submitted as necessary. This document is to be read consistently with the qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms found in the CBPR Intake Questionnaire.

(Please note the English version of the Acts described in the following table is not official.)

Notice

Assessment Purpose – *To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used.*

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If YES, the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline.	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree (3) If there are discrepancies between the Privacy Policy and the contract entered into by and between the Personal information Controller and Data Subjects, what is beneficial to the Data Subject prevails. (4) The PIPC may prepare the Privacy Policy Guidelines and encourage the Personal information Controller to comply with such guidelines. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy)

	• States an effective date of Privacy Statement publication. Where Applicant answers NO to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30. (2) The Personal information Controller shall post continuously the Privacy Policy established or modified pursuant to Article 30(2) of the Act on its website. (3) If it is not possible to post on the website pursuant to paragraph (2), the Personal information Controller shall make public the Privacy Policy established or modified in a way of more than one of the following subparagraphs: 1. Posting at easily noticeable places of the Personal information Controller's, etc.; 2. Publishing at the Official Gazette (only in case the Personal information Controller is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the City and Province where the Personal information Controller's is located. 3. Publishing at a periodical, newsletter, PR magazine or invoice to be published under the same title more than twice a year and distributed to Data Subjects on a continual basis; and/or 4. Delivering to the Data Subject the paper-based agreement entered into between the Personal information Controller and the Data Subject so as to supply goods and/or services.
1.a) Does this privacy statement describe how personal information is collected?	If YES, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant.	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable);

	• the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If NO, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree (3) If there are discrepancies between the Privacy Policy and the contract entered into by and between the Personal information Controller and Data Subjects, what is beneficial to the Data Subject prevails. (4) The PIPC may prepare the Privacy Policy Guidelines and encourage the Personal information Controller to comply with such guidelines. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30.
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers NO and does not identify an applicable qualification set out below, the Accountability Agent	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and

	must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree (3) If there are discrepancies between the Privacy Policy and the contract entered into by and between the Personal information Controller and Data Subjects, what is beneficial to the Data Subject prevails. (4) The PIPC may prepare the Privacy Policy Guidelines and encourage the Personal information Controller to comply with such guidelines. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30.
1. c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree.

	Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree (3) If there are discrepancies between the Privacy Policy and the contract entered into by and between the Personal information Controller and Data Subjects, what is beneficial to the Data Subject prevails. (4) The PIPC may prepare the Privacy Policy Guidelines and encourage the Personal information Controller to comply with such guidelines. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30.
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree.

	Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree (3) If there are discrepancies between the Privacy Policy and the contract entered into by and between the Personal information Controller and Data Subjects, what is beneficial to the Data Subject prevails. (4) The PIPC may prepare the Privacy Policy Guidelines and encourage the Personal information Controller to comply with such guidelines. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30.
1. e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree

	inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(3) If there are discrepancies between the Privacy Policy and the contract entered into by and between the Personal information Controller and Data Subjects, what is beneficial to the Data Subject prevails. (4) The PIPC may prepare the Privacy Policy Guidelines and encourage the Personal information Controller to comply with such guidelines. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30.
1. f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers YES, the Accountability Agent must verify that the Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information Where the Applicant answers NO and does not identify an	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree (3) If there are discrepancies between the Privacy Policy and the contract entered into by and between the Personal information Controller and Data Subjects, what is beneficial to the Data Subject prevails.

	applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(4) The PIPC may prepare the Privacy Policy Guidelines and encourage the Personal information Controller to comply with such guidelines. Article 35 (Access to Personal Information) (1) Data Subjects may demand access to their own personal information being processed by the Personal information Controller, to the relevant Personal information Controller. (2) Notwithstanding paragraph (1), when any Data Subject intends to request access to his/her own personal information to the public institution, the Data Subject may request directly to the said institution, or indirectly through the PIPCas stipulated by presidential decree. (3) The Personal information Controller shall, when it is requested access pursuant to paragraphs (1) and (2), ensure the Data Subjects have access to the relevant personal information within the period as stipulated by presidential decree. In such case, if there is any justifiable ground not to allow access within such period, the Personal information Controller may postpone access after notifying the relevant Data Subjects of the said reason. If the said reason expires, access is to be allowed without delay. (4) In case where any of the following subparagraphs is applicable, the Personal information Controller may restrict or deny access after notifying Data Subjects of the reason: 1. Where access is prohibited or restricted by law; 2. Where access may probably cause damage to the life or body of others, or unfairly infringe properties and other benefits of others; or 3. Where the public institutions have grave difficulties in carrying out any of the following Items: a. Imposition, collection or repayment of taxes; b. Evaluation of academic achievements or admission affairs at schools established by the Elementary and Middle Education Act and the Higher Education Act, at lifelong educational facilities established by the Lifelong Education Act, and other higher educational institutions established by other laws;

		c. Testing and qualification examination regarding academic competence, technical capability and employment; d. Ongoing evaluation or decision-making in relation to compensation or grant assessment; or e. Ongoing auditing and examination under other laws. (5) Necessary matters in relation to the method and procedure of request of access, access restriction, notification, etc. pursuant to paragraphs (1) through (4) shall be stipulated by presidential decree. Article 36 (Rectification or Deletion of Personal information) (1) The Data Subjects, who have accessed their own personal information pursuant to Article 35, may demand the correction or deletion of such personal information to the Personal information Controller; provided, however, that the deletion is not allowed where the said personal information is listed as subject to collection by other laws and regulations. (2) Upon receiving a demand from a Data Subject pursuant to paragraph (1), the Personal information Controller shall, without delay, review the personal information in question, and take necessary measures to correct or delete as demanded by the said Data Subject unless specific procedures are stipulated by other laws and regulations. Then the Personal information Controller shall notify the relevant Data Subject of the result. (3) The Personal information Controller shall take measures to preclude the possibility of restoring or recovering deleted personal information in case of deletion pursuant to paragraph (2). (4) When a request of a Data Subject applies to the proviso of paragraph (1), the Personal information Controller shall, without delay, notify the relevant Data Subjects of its content. (5) The Personal information Controller, while investigating the personal information in question pursuant to paragraph (2) may, if necessary, demand the evidence necessary to confirm the correction and deletion of the personal information to the relevant Data Subjects. (6) Necessary matters for the method and procedure for a demanded rectification and deletion, notification pursuant to paragraphs (1), (2) and (4) shall be followed as stipulated by presidential decree.

		Article 37 (Suspension of Processing of Personal information, etc.) (1) Data Subjects may request the Personal information Controller to suspend the processing of their own personal information. In case the Personal information Controller is a public institution, the Data Subjects may request the suspension of processing of their personal information contained in the personal information files subject to being registered pursuant to Article 32. (2) Upon receiving a demand pursuant to paragraph (1), the Personal information Controller shall, without delay, suspend the processing of the said personal information in whole or in part as demanded by the Data Subject; provided, however, that, where any of the following subparagraphs is applicable, the Personal information Controller may reject the demand of the said Data Subject: 1. Where it is specifically stipulated by law or it is inevitably necessary to observe obligations under relevant laws and regulations; 2. Where it may probably cause damage to the life or body of others, or improper violation of properties and benefits of others; 3. Where the public institution cannot carry out its work as prescribed by other laws without processing the personal information in question; or 4. Where it is difficult to fulfill a contract entered by and between the Personal information Controller and the Data Subject without processing the personal information and where the Data Subject fails to express explicitly the termination of the said contract. (3) The Personal information Controller shall, when rejecting the demand pursuant to the proviso of paragraph (2)notify the Data Subject of the reason without delay. (4) The Personal information Controller shall, without delay, take necessary measures including destruction of the relevant personal information when suspending the processing of personal information as demanded by a Data Subject. (5) Necessary matters in relation for the method and procedure of the demand or rejection of suspension of processing, notification, etc. pursuant to paragraphs (1) through (3) shall be stipulated by presidential decree. Article 38 (Method and Procedure for Exercising of Rights) (1) Data Subject may delegate to their attorneys the right to access pursuant to Article 35, correction or deletion pursuant to Article 36, demand of suspension of processing pursuant to Article 37 (hereinafter

		referred to collectively as "access demand") in writing or in a manner and procedure as stipulated by presidential decree. (2) The legal representative of a minor of age below 14 may request the access demand for the minor to the Personal information Controller. (3) The Personal information Controller may demand the fee and postage (only in the case of request mailing of the photocopy) to the person requesting the access, etc. demand as stipulated by presidential decree. (4) The Personal information Controller shall prepare and disclose in detail the method and procedure to enable the Data Subjects to request the access demand. (5) The Personal information Controller shall prepare, and guide, the necessary procedure for Data Subjects to raise objections against the rejection to the access demand requested by the said Data Subjects. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30.
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals.	Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects;

that such information is being collected?	Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other.	Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of

	Where the Applicant answers NO and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent.
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers NO and does not identify an applicable qualification set out on part II of	Article 17 (Provision of Personal information) (1) The Personal information Controller may provide (or share, hereinafter the same applies) the personal information of Data Subjects to a third party in cases applicable to any of the following subparagraphs: 1. Where the consent of the Data Subject is obtained; or 2. Where personal information is provided within the scope of purposes for which personal information is collected under subparagraphs 2, 3 and 5 of Article 15(1); (2) The Personal information Controller shall inform Data Subjects of the following when it obtains consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The recipient of the personal information; 2. The purpose of use of the personal information of the said recipient; 3. Items of personal information to be provided; 4. The use and retention period of the said recipient; and

	the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	5. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. (3) When a Personal information Controller provides personal information to a third party located overseas, the Personal information Controller shall first inform the Data Subjects of any of the subparagraphs of paragraph (2), and obtain consent from them. The Personal information Controller shall not enter into a contract for the cross-border transfer of personal information in violation of this Act. Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (2) A Personal information Controller who entrusts the processing of personal information to a third party pursuant to paragraph (1) (hereinafter the “entrustor”) shall disclose the persons who are or have been entrusted (hereinafter the “entrustee”) as well as the entrusted tasks related to the personal information to ensure that the Data Subjects may easily recognize it at any time in such a manner as stipulated by presidential decree. (3) The entrustor shall, in case of entrusting tasks related to public relations or the solicitation of goods or services, inform Data Subjects of the entrusted tasks and also the entrustee in such a manner as stipulated by presidential decree. The same shall apply when the entrusted tasks or entrustee has been changed. (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information.

		(5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. (7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee.

Collection Limitation

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. 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*

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
5. How do you obtain personal information: 5. a) Directly from the individual? 5. b) From third parties collecting on your behalf? 5. c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers YES to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	Article 3 (Personal information Protection Principles) (1) The Personal information Controller shall explicitly specify the purpose of processing the personal information, and shall lawfully and fairly collect the minimum of such personal information to the extent necessary for such purposes. Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with

		the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. Article 20 (Notification of the Sources of Collection, etc. Other Than Data Subject) (1) When a Personal information Controller processes personal information collected from sources other than Data Subjects, the Personal information Controller shall immediately notify such Data Subjects of everything stated in the following subparagraphs upon their demand: 1. The source of the collected personal information; 2. The purpose of processing the personal information; and 3. The fact that a Data Subject is entitled to demand suspension of the processing of the personal information. Article 22 (Methods of Obtaining Consent) (5) The Personal information Controller shall, when required to obtain consent in accordance with this Act with regards to children below the age of 14 years, obtain consent from their legal representatives. In such case, the minimum personal information necessary to obtain consent from the legal representatives may be collected directly from such children without the consent of their legal representatives. Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs:

		1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (2) A Personal information Controller who entrusts the processing of personal information to a third party pursuant to paragraph (1) (hereinafter the "entrustor") shall disclose the persons who are or have been entrusted (hereinafter the "entrustee") as well as the entrusted tasks related to the personal information to ensure that the Data Subjects may easily recognize it at any time in such a manner as stipulated by presidential decree.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers YES and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each	Article 3 (Personal information Protection Principles) (1) The Personal information Controller shall explicitly specify the purpose of processing the personal information, and shall lawfully and fairly collect the minimum of such personal information to the extent necessary for such purposes. (2) The Personal information Controller shall appropriately process personal information to the extent necessary to attain the personal information processing purposes, and shall not use them for any other purposes. Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the

	identified use with the stated purpose of collection Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers NO, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent.
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information?	Where the Applicant answers YES, the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers NO, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	Article 3 (Personal information Protection Principles) (1) The Personal information Controller shall explicitly specify the purpose of processing the personal information, and shall lawfully and fairly collect the minimum of such personal information to the extent necessary for such purposes. Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects;

Where YES, describe.		5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. Article 59 (Prohibited Activities) No one who processes or had processed personal information shall engage in any of the following: 1. Obtain personal information or obtain the consent to personal information processing in a fraudulent, improper or unfair manner;

Uses of Personal Information

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific 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 applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If	Where the Applicant answers YES, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below.	Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3). (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, the Personal information Controller may use personal information for a purpose other than the intended one, or provide it to a third party, unless it likely infringes upon unfairly the interests of Data Subjects or a third party; provided, however, that subparagraphs 5 through 9 are applicable only to public institutions. 1. Where separate consent is obtained from Data Subjects; 2. Where special provisions exist in laws; 3. Where it is deemed explicitly necessary for the protection of, from impending danger, the life, body or economic profits of the Data Subject or a third party in case that the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; 4. Where personal information is provided in a manner that keeps individuals unidentifiable necessarily for the purposes of statistics and academic research, etc.; 5. Where it is impossible to carry out the work under its jurisdiction as stated in other laws unless the Personal information Controller uses personal information for a purpose other than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution of the Commission;

necessary, provide a description in the space below.		6. Where it is necessary to provide personal information to a foreign government or international organization so as to abide by a treaty obligation or other international convention; 7. Where it is necessary to investigate crimes, and launch and sustain a prosecution; 8. Where it is necessary for the court to perform its judicial affairs; or 9. Where it is necessary to execute a punishment, take custody, or for protective disposition. Article 19 (Limitations on the Use and Provision of Personal information on the Part of the Recipient) A person who receives personal information from a Personal information Controller shall not use such personal information for purposes other than the intended one, or shall not provide it to a third party except in cases applicable to any of the following subparagraphs: 1. Where separate consent is obtained from Data Subjects; or 2. Where special provisions exist in other laws. Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with

		the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual?	Where the Applicant answers NO to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on	Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3). (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, the Personal information Controller may use personal information for a purpose other than the intended one, or provide it to a third party, unless it likely infringes upon unfairly the interests of Data Subjects or a third party; provided, however, that subparagraphs 5 through 9 are applicable only to public institutions. 1. Where separate consent is obtained from Data Subjects; 2. Where special provisions exist in laws; 3. Where it is deemed explicitly necessary for the protection of, from impending danger, the life, body or economic profits of the Data Subject or a third party in case that the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; 4. Where personal information is provided in a manner that keeps individuals unidentifiable necessarily for the purposes of statistics and academic research, etc.;

9.b) Compelled by applicable laws?	express consent of the individual (9.a), such as: • Online at point of • collection • Via e-mail • Via preference/profile • page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law.	5. Where it is impossible to carry out the work under its jurisdiction as stated in other laws unless the Personal information Controller uses personal information for a purpose other than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution of the Commission; 6. Where it is necessary to provide personal information to a foreign government or international organization so as to abide by a treaty obligation or other international convention; 7. Where it is necessary to investigate crimes, and launch and sustain a prosecution; 8. Where it is necessary for the court to perform its judicial affairs; or 9. Where it is necessary to execute a punishment, take custody, or for protective disposition. Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall

	Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent.
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other Personal information Controllers? If YES, describe.	Where the Applicant answers YES in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other Personal information Controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law.	Article 17 (Provision of Personal information) (1) The Personal information Controller may provide (or share, hereinafter the same applies) the personal information of Data Subjects to a third party in cases applicable to any of the following subparagraphs: 1. Where the consent of the Data Subject is obtained; or 2. Where personal information is provided within the scope of purposes for which personal information is collected under subparagraphs 2, 3 and 5 of Article 15(1); (2) The Personal information Controller shall inform Data Subjects of the following when it obtains consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The recipient of the personal information; 2. The purpose of use of the personal information of the said recipient; 3. Items of personal information to be provided; 4. The use and retention period of the said recipient; and 5. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. (3) When a Personal information Controller provides personal information to a third party located overseas, the Personal information Controller shall first inform the Data Subjects of any of the subparagraphs of paragraph (2), and obtain consent from them. The Personal

	Also, the Accountability Agent must require the Applicant to identify: each type of data disclosed or transferred; the corresponding stated purpose of collection for each type of disclosed data; and the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	information Controller shall not enter into a contract for the cross-border transfer of personal information in violation of this Act. Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3).
11. Do you transfer personal information to personal information processors? If YES, describe.		Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (2) A Personal information Controller who entrusts the processing of personal information to a third party pursuant to paragraph (1) (hereinafter the "entrustor") shall disclose the persons who are or have been entrusted (hereinafter the "entrustee") as well as the

		entrusted tasks related to the personal information to ensure that the Data Subjects may easily recognize it at any time in such a manner as stipulated by presidential decree. (3) The entrustor shall, in case of entrusting tasks related to public relations or the solicitation of goods or services, inform Data Subjects of the entrusted tasks and also the entrustee in such a manner as stipulated by presidential decree. The same shall apply when the entrusted tasks or entrustee has been changed. (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. (5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. (7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee.
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible		Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3). (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, the Personal information Controller may use personal information for a purpose other than the intended one, or provide it to a third party, unless it likely infringes upon unfairly the interests of Data Subjects or a third party; provided, however, that subparagraphs 5 through 9 are applicable only to public institutions. 1. Where separate consent is obtained from Data Subjects; 2. Where special provisions exist in laws; 3. Where it is deemed explicitly necessary for the protection of, from impending danger, the life, body or economic profits of the Data Subject or a third party in case that the Data

or related purpose? If YES, describe.		Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; 4. Where personal information is provided in a manner that keeps individuals unidentifiable necessarily for the purposes of statistics and academic research, etc.; 5. Where it is impossible to carry out the work under its jurisdiction as stated in other laws unless the Personal information Controller uses personal information for a purpose other than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution of the Commission; 6. Where it is necessary to provide personal information to a foreign government or international organization so as to abide by a treaty obligation or other international convention; 7. Where it is necessary to investigate crimes, and launch and sustain a prosecution; 8. Where it is necessary for the court to perform its judicial affairs; or 9. Where it is necessary to execute a punishment, take custody, or for protective disposition. Article 19 (Limitations on the Use and Provision of Personal information on the Part of the Recipient) A person who receives personal information from a Personal information Controller shall not use such personal information for purposes other than the intended one, or shall not provide it to a third party except in cases applicable to any of the following subparagraphs: 1. Where separate consent is obtained from Data Subjects; or 2. Where special provisions exist in other laws.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of	Where applicant answers NO to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers YES to 13.a, the Accountability Agent must	Article 17 (Provision of Personal information) (1) The Personal information Controller may provide (or share, hereinafter the same applies) the personal information of Data Subjects to a third party in cases applicable to any of the following subparagraphs: 1. Where the consent of the Data Subject is obtained; or 2. Where personal information is provided within the scope of purposes for which personal information is collected under subparagraphs 2, 3 and 5 of Article 15(1); (2) The Personal information Controller shall inform Data Subjects of the following when it obtains consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The

the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers YES to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual.	recipient of the personal information; 2. The purpose of use of the personal information of the said recipient; 3. Items of personal information to be provided; 4. The use and retention period of the said recipient; and 5. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. (3) When a Personal information Controller provides personal information to a third party located overseas, the Personal information Controller shall first inform the Data Subjects of any of the subparagraphs of paragraph (2), and obtain consent from them. The Personal information Controller shall not enter into a contract for the cross-border transfer of personal information in violation of this Act. Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (2) A Personal information Controller who entrusts the processing of personal information to a third party pursuant to paragraph (1) (hereinafter the "entrustor") shall disclose the persons who are or have been entrusted (hereinafter the "entrustee") as well as the entrusted tasks related to the personal information to ensure that the Data Subjects may easily recognize it at any time in such a manner as stipulated by presidential decree. (3) The entrustor shall, in case of entrusting tasks related to public relations or the solicitation of goods or services, inform Data Subjects of the entrusted tasks and also the entrustee in such a manner as stipulated by presidential decree. The same shall apply when the entrusted tasks or entrustee has been changed. (5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party.

	Where the Applicant answers YES to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement or permission. Where the Applicant answers NO to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	

Choice

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations.*

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection •Via e-mail •Via preference/profile page •Via telephone •Via postal mail, or •Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the	Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope.

	purpose of collection is clearly stated. Where the Applicant answers NO, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	(2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. Article 22 (Methods of Obtaining Consent) (1) When a Personal information Controller obtains consent from Data Subjects (including their legal representatives as stated in paragraph (5), hereinafter the same applies to this Article) with respect to personal information processing under this Act, the Personal information Controller shall inform the Data Subjects of the fact by separating the matters requiring consent and helping the Data Subjects to recognize it explicitly, and obtain their consent thereof, respectively. (2) When a Personal information Controller obtains consent from Data Subjects with respect to personal information processing in accordance with Articles 15(1)i, 17(1)i and 24(1)i, the Personal information Controller shall segregate the personal information which needs the Data Subjects' consent to process, from the personal information which needs no consent when entering into a contract with the Data Subjects. In such case, the burden of proof that no consent is required in processing the personal information shall be borne by the Personal information Controller. (3) The Personal information Controller shall, when intending to obtain Data Subjects' consent to personal information processing for the purpose of soliciting the purchase or promoting the goods and services thereof, inform the Data Subjects of the fact by helping the Data Subjects to recognize it explicitly, and obtain their consent thereof. (4) The Personal information Controller shall not refuse the provision of goods or services to the Data Subjects on the ground that the Data Subjects would not consent to the matter eligible for selective consent pursuant to paragraph (2), or (3) and Article 18(2)i.

		(5) The Personal information Controller shall, when required to obtain consent in accordance with this Act with regards to children below the age of 14 years, obtain consent from their legal representatives. In such case, the minimum personal information necessary to obtain consent from the legal representatives may be collected directly from such children without the consent of their legal representatives.
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for	Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent.

	subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a	Article 22 (Methods of Obtaining Consent) (1) When a Personal information Controller obtains consent from Data Subjects (including their legal representatives as stated in paragraph (5), hereinafter the same applies to this Article) with respect to personal information processing under this Act, the Personal information Controller shall inform the Data Subjects of the fact by separating the matters requiring consent and helping the Data Subjects to recognize it explicitly, and obtain their consent thereof, respectively. (2) When a Personal information Controller obtains consent from Data Subjects with respect to personal information processing in accordance with Articles 15(1)i, 17(1)i and 24(1)i, the Personal information Controller shall segregate the personal information which needs the Data Subjects' consent to process, from the personal information which needs no consent when entering into a contract with the Data Subjects. In such case, the burden of proof that no consent is required in processing the personal information shall be borne by the Personal information Controller. (3) The Personal information Controller shall, when intending to obtain Data Subjects' consent to personal information processing for the purpose of soliciting the purchase or promoting the goods and services thereof, inform the Data Subjects of the fact by helping the Data Subjects to recognize it explicitly, and obtain their consent thereof. (4) The Personal information Controller shall not refuse the provision of goods or services to the Data Subjects on the ground that the Data Subjects would not consent to the matter eligible for selective consent pursuant to paragraph (2), or (3) and Article 18(2)i. (5) The Personal information Controller shall, when required to obtain consent in accordance with this Act with regards to children below the age of 14 years, obtain consent from their legal representatives. In such case, the minimum personal information necessary to obtain consent from the legal representatives may be collected directly from such children without the consent of their legal representatives.

	mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information.	Article 17 (Provision of Personal information) (1) The Personal information Controller may provide (or share, hereinafter the same applies) the personal information of Data Subjects to a third party in cases applicable to any of the following subparagraphs: 1. Where the consent of the Data Subject is obtained; or 2. Where personal information is provided within the scope of purposes for which personal information is collected under subparagraphs 2, 3 and 5 of Article 15(1); (2) The Personal information Controller shall inform Data Subjects of the following when it obtains consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The recipient of the personal information; 2. The purpose of use of the personal information of the said recipient; 3. Items of personal information to be provided; 4. The use and retention period of the said recipient; and 5. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. (3) When a Personal information Controller provides personal information to a third party located overseas, the Personal information Controller shall first inform the Data Subjects of any of the subparagraphs of paragraph (2), and obtain consent from them. The Personal information Controller shall not enter into a contract for the cross-border transfer of personal information in violation of this Act. Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3). (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, the Personal information Controller may use personal information for a purpose other than the

	Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner , or compatible with that for which the information was collected.] Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the	intended one, or provide it to a third party, unless it likely infringes upon unfairly the interests of Data Subjects or a third party; provided, however, that subparagraphs 5 through 9 are applicable only to public institutions. 1. Where separate consent is obtained from Data Subjects;

	disclosure of their personal information must be provided.	
17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree Article 22 (Methods of Obtaining Consent) (1) When a Personal information Controller obtains consent from Data Subjects (including their legal representatives as stated in paragraph (5), hereinafter the same applies to this Article) with respect to personal information processing under this Act, the Personal information Controller shall inform the Data Subjects of the fact by separating the matters requiring consent and helping the Data Subjects to recognize it explicitly, and obtain their consent thereof, respectively. (2) When a Personal information Controller obtains consent from Data Subjects with respect to personal information processing in accordance with Articles 15(1)i, 17(1)i and 24(1)i, the Personal information Controller shall segregate the personal information which needs the Data Subjects' consent to process, from the personal information which needs no consent when entering into a contract with the Data Subjects. In such case, the burden

		of proof that no consent is required in processing the personal information shall be borne by the Personal information Controller. (3) The Personal information Controller shall, when intending to obtain Data Subjects' consent to personal information processing for the purpose of soliciting the purchase or promoting the goods and services thereof, inform the Data Subjects of the fact by helping the Data Subjects to recognize it explicitly, and obtain their consent thereof. (4) The Personal information Controller shall not refuse the provision of goods or services to the Data Subjects on the ground that the Data Subjects would not consent to the matter eligible for selective consent pursuant to paragraph (2), or (3) and Article 18(2)i. (5) The Personal information Controller shall, when required to obtain consent in accordance with this Act with regards to children below the age of 14 years, obtain consent from their legal representatives. In such case, the minimum personal information necessary to obtain consent from the legal representatives may be collected directly from such children without the consent of their legal representatives. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30. (2) The Personal information Controller shall post continuously the Privacy Policy established or modified pursuant to Article 30(2) of the Act on its website. (3) If it is not possible to post on the website pursuant to paragraph (2), the Personal information Controller shall make public the Privacy Policy established or modified in a way of more than one of the following subparagraphs: 1. Posting at easily noticeable places of the Personal information Controller's , etc.;

		2. Publishing at the Official Gazette (only in case the Personal information Controller is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the City and Province where the Personal information Controller's is located. 3. Publishing at a periodical, newsletter, PR magazine or invoice to be published under the same title more than twice a year and distributed to Data Subjects on a continual basis; and/or 4. Delivering to the Data Subject the paper-based agreement entered into between the Personal information Controller and the Data Subject so as to supply goods and/or services.
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers NO, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree Article 22 (Methods of Obtaining Consent) (1) When a Personal information Controller obtains consent from Data Subjects (including their legal representatives as stated in paragraph (5), hereinafter the same applies to this Article) with respect to personal information processing under this Act, the Personal information Controller shall inform the

		Data Subjects of the fact by separating the matters requiring consent and helping the Data Subjects to recognize it explicitly, and obtain their consent thereof, respectively. (2) When a Personal information Controller obtains consent from Data Subjects with respect to personal information processing in accordance with Articles 15(1)i, 17(1)i and 24(1)i, the Personal information Controller shall segregate the personal information which needs the Data Subjects' consent to process, from the personal information which needs no consent when entering into a contract with the Data Subjects. In such case, the burden of proof that no consent is required in processing the personal information shall be borne by the Personal information Controller. (3) The Personal information Controller shall, when intending to obtain Data Subjects' consent to personal information processing for the purpose of soliciting the purchase or promoting the goods and services thereof, inform the Data Subjects of the fact by helping the Data Subjects to recognize it explicitly, and obtain their consent thereof. (4) The Personal information Controller shall not refuse the provision of goods or services to the Data Subjects on the ground that the Data Subjects would not consent to the matter eligible for selective consent pursuant to paragraph (2), or (3) and Article 18(2)i. (5) The Personal information Controller shall, when required to obtain consent in accordance with this Act with regards to children below the age of 14 years, obtain consent from their legal representatives. In such case, the minimum personal information necessary to obtain consent from the legal representatives may be collected directly from such children without the consent of their legal representatives. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and

		3. Matters in relation to safety measures of Data Subject to Article 30. (2) The Personal information Controller shall post continuously the Privacy Policy established or modified pursuant to Article 30(2) of the Act on its website. (3) If it is not possible to post on the website pursuant to paragraph (2), the Personal information Controller shall make public the Privacy Policy established or modified in a way of more than one of the following subparagraphs: 1. Posting at easily noticeable places of the Personal information Controller's , etc.; 2. Publishing at the Official Gazette (only in case the Personal information Controller is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the City and Province where the Personal information Controller's is located. 3. Publishing at a periodical, newsletter, PR magazine or invoice to be published under the same title more than twice a year and distributed to Data Subjects on a continual basis; and/or 4. Delivering to the Data Subject the paper-based agreement entered into between the Personal information Controller and the Data Subject so as to supply goods and/or services.
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree.

Where YES, describe.	relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	(2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree Article 22 (Methods of Obtaining Consent) (1) When a Personal information Controller obtains consent from Data Subjects (including their legal representatives as stated in paragraph (5), hereinafter the same applies to this Article) with respect to personal information processing under this Act, the Personal information Controller shall inform the Data Subjects of the fact by separating the matters requiring consent and helping the Data Subjects to recognize it explicitly, and obtain their consent thereof, respectively. (2) When a Personal information Controller obtains consent from Data Subjects with respect to personal information processing in accordance with Articles 15(1)i, 17(1)i and 24(1)i, the Personal information Controller shall segregate the personal information which needs the Data Subjects' consent to process, from the personal information which needs no consent when entering into a contract with the Data Subjects. In such case, the burden of proof that no consent is required in processing the personal information shall be borne by the Personal information Controller. (3) The Personal information Controller shall, when intending to obtain Data Subjects' consent to personal information processing for the purpose of soliciting the purchase or promoting the goods and services thereof, inform the Data Subjects of the fact by helping the Data Subjects to recognize it explicitly, and obtain their consent thereof. (4) The Personal information Controller shall not refuse the provision of goods or services to the Data Subjects on the ground that the Data Subjects would not consent to the matter eligible for selective consent pursuant to paragraph (2), or (3) and Article 18(2)i. (5) The Personal information Controller shall, when required to obtain consent in accordance with this Act with regards to children below the age of 14 years, obtain consent from their legal representatives. In such case, the minimum personal information

		necessary to obtain consent from the legal representatives may be collected directly from such children without the consent of their legal representatives. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30. (2) The Personal information Controller shall post continuously the Privacy Policy established or modified pursuant to Article 30(2) of the Act on its website. (3) If it is not possible to post on the website pursuant to paragraph (2), the Personal information Controller shall make public the Privacy Policy established or modified in a way of more than one of the following subparagraphs: 1. Posting at easily noticeable places of the Personal information Controller's , etc.; 2. Publishing at the Official Gazette (only in case the Personal information Controller is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the City and Province where the Personal information Controller's is located. 3. Publishing at a periodical, newsletter, PR magazine or invoice to be published under the same title more than twice a year and distributed to Data Subjects on a continual basis; and/or 4. Delivering to the Data Subject the paper-based agreement entered into between the Personal information Controller and the Data Subject so as to supply goods and/or services.

20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. (2) The Personal information Controller shall, when stablishing or modifying the Privacy Policy, disclose the contents so that Data Subjects may easily recognize it in such a manner as prescribed by presidential decree Article 22 (Methods of Obtaining Consent) (1) When a Personal information Controller obtains consent from Data Subjects (including their legal representatives as stated in paragraph (5), hereinafter the same applies to this Article) with respect to personal information processing under this Act, the Personal information Controller shall inform the Data Subjects of the fact by separating the matters requiring consent and helping the Data Subjects to recognize it explicitly, and obtain their consent thereof, respectively. (2) When a Personal information Controller obtains consent from Data Subjects with respect to personal information processing in accordance with Articles 15(1)i, 17(1)i and 24(1)i, the Personal information Controller shall segregate the personal information which needs the Data Subjects' consent to process, from the personal information which needs no consent when entering into a contract with the Data Subjects. In such case, the burden of proof that no consent is required in processing the personal information shall be borne by the Personal information Controller.

		(3) The Personal information Controller shall, when intending to obtain Data Subjects' consent to personal information processing for the purpose of soliciting the purchase or promoting the goods and services thereof, inform the Data Subjects of the fact by helping the Data Subjects to recognize it explicitly, and obtain their consent thereof. (4) The Personal information Controller shall not refuse the provision of goods or services to the Data Subjects on the ground that the Data Subjects would not consent to the matter eligible for selective consent pursuant to paragraph (2), or (3) and Article 18(2)i. (5) The Personal information Controller shall, when required to obtain consent in accordance with this Act with regards to children below the age of 14 years, obtain consent from their legal representatives. In such case, the minimum personal information necessary to obtain consent from the legal representatives may be collected directly from such children without the consent of their legal representatives. ENFORCEMENT DECREE Article 31 (Establishment and Disclosure of Privacy Policy) (1) "Other matters as stated in the Presidential Decree" in Article 30(1)vi shall mean the matters of following subparagraphs: 1. Items of personal information to be processed; 2. Matters in relation to destruction of personal information; and 3. Matters in relation to safety measures of Data Subject to Article 30. (2) The Personal information Controller shall post continuously the Privacy Policy established or modified pursuant to Article 30(2) of the Act on its website. (3) If it is not possible to post on the website pursuant to paragraph (2), the Personal information Controller shall make public the Privacy Policy established or modified in a way of more than one of the following subparagraphs: 1. Posting at easily noticeable places of the Personal information Controller's , etc.;

		2. Publishing at the Official Gazette (only in case the Personal information Controller is the public institution), or general daily newspaper, weekly newsmagazine or Internet media subject to Articles 2 i a. and c. and 2 ii of the Act for the Promotion of Newspapers, etc. circulating mainly in over the City and Province where the Personal information Controller's is located. 3. Publishing at a periodical, newsletter, PR magazine or invoice to be published under the same title more than twice a year and distributed to Data Subjects on a continual basis; and/or 4. Delivering to the Data Subject the paper-based agreement entered into between the Personal information Controller and the Data Subject so as to supply goods and/or services.

Integrity of personal Information

Assessment Purpose - *The questions in this section are directed towards ensuring that the Personal information Controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and	Article 3 (Personal information Protection Principles) (3) The Personal information Controller shall ensure that the personal information is accurate, complete and up to date to the extent necessary to attain the purpose of processing the personal information. (5) The Personal information Controller shall disclose the privacy policy and other matters related to the processing of the personal information and shall ensure the relevant rights of the Data Subject such as the right to access to the personal information, etc. Article 35 (Access to Personal information) (1) Data Subjects may demand access to their own personal information being processed by the Personal information Controller, to the relevant Personal information Controller. (2) Notwithstanding paragraph (1), when any Data Subject intends to request access to his/her own personal information to the public institution, the Data Subject may request directly to the said institution, or indirectly through the PIPCas stipulated by presidential decree. (3) The Personal information Controller shall, when it is requested access pursuant to paragraphs (1) and (2), ensure the Data Subjects have access to the relevant personal information within the period as stipulated by presidential decree. In such case, if there is any justifiable ground not to allow access within such period, the Personal information Controller may postpone access after notifying the relevant Data Subjects of the said reason. If the said reason expires, access is to be allowed without delay.

	complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	(4) In case where any of the following subparagraphs is applicable, the Personal information Controller may restrict or deny access after notifying Data Subjects of the reason: 1. Where access is prohibited or restricted by law; 2. Where access may probably cause damage to the life or body of others, or unfairly infringe properties and other benefits of others; or 3. Where the public institutions have grave difficulties in carrying out any of the following Items: Article 36 (Rectification or Deletion of Personal information) (1) The Data Subjects, who have accessed their own personal information pursuant to Article 35, may demand the correction or deletion of such personal information to the Personal information Controller; provided, however, that the deletion is not allowed where the said personal information is listed as subject to collection by other laws and regulations. (2) Upon receiving a demand from a Data Subject pursuant to paragraph (1), the Personal information Controller shall, without delay, review the personal information in question, and take necessary measures to correct or delete as demanded by the said Data Subject unless specific procedures are stipulated by other laws and regulations. Then the Personal information Controller shall notify the relevant Data Subject of the result. (3) The Personal information Controller shall take measures to preclude the possibility of restoring or recovering deleted personal information in case of deletion pursuant to paragraph (2). (4) When a request of a Data Subject applies to the proviso of paragraph (1), the Personal information Controller shall, without delay, notify the relevant Data Subjects of its content. (5) The Personal information Controller, while investigating the personal information in question pursuant to paragraph (2)may, if necessary, demand the evidence necessary to confirm the correction and deletion of the personal information to the relevant Data Subjects.

22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	Article 3 (Personal information Protection Principles) (3) The Personal information Controller shall ensure that the personal information is accurate, complete and up to date to the extent necessary to attain the purpose of processing the personal information. (5) The Personal information Controller shall disclose the privacy policy and other matters related to the processing of the personal information and shall ensure the relevant rights of the Data Subject such as the right to access to the personal information, etc. Article 35 (Access to Personal information) (1) Data Subjects may demand access to their own personal information being processed by the Personal information Controller, to the relevant Personal information Controller. (2) Notwithstanding paragraph (1), when any Data Subject intends to request access to his/her own personal information to the public institution, the Data Subject may request directly to the said institution, or indirectly through the PIPCas stipulated by presidential decree. (3) The Personal information Controller shall, when it is requested access pursuant to paragraphs (1) and (2), ensure the Data Subjects have access to the relevant personal information within the period as stipulated by presidential decree. In such case, if there is any justifiable ground not to allow access within such period, the Personal information Controller may postpone access after notifying the relevant Data Subjects of the said reason. If the said reason expires, access is to be allowed without delay. (4) In case where any of the following subparagraphs is applicable, the Personal information Controller may restrict or deny access after notifying Data Subjects of the reason: 1. Where access is prohibited or restricted by law; 2. Where access may probably cause damage to the life or body of others, or unfairly infringe properties and other benefits of others; or 3. Where the public institutions have grave difficulties in carrying out any of the following Items:

		Article 36 (Rectification or Deletion of Personal information) (1) The Data Subjects, who have accessed their own personal information pursuant to Article 35, may demand the correction or deletion of such personal information to the Personal information Controller; provided, however, that the deletion is not allowed where the said personal information is listed as subject to collection by other laws and regulations. (2) Upon receiving a demand from a Data Subject pursuant to paragraph (1), the Personal information Controller shall, without delay, review the personal information in question, and take necessary measures to correct or delete as demanded by the said Data Subject unless specific procedures are stipulated by other laws and regulations. Then the Personal information Controller shall notify the relevant Data Subject of the result. (3) The Personal information Controller shall take measures to preclude the possibility of restoring or recovering deleted personal information in case of deletion pursuant to paragraph (2). (4) When a request of a Data Subject applies to the proviso of paragraph (1), the Personal information Controller shall, without delay, notify the relevant Data Subjects of its content. (5) The Personal information Controller, while investigating the personal information in question pursuant to paragraph (2)may, if necessary, demand the evidence necessary to confirm the correction and deletion of the personal information to the relevant Data Subjects.
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service	Article 3 (Personal information Protection Principles) (3) The Personal information Controller shall ensure that the personal information is accurate, complete and up to date to the extent necessary to attain the purpose of processing the personal information. (5) The Personal information Controller shall disclose the privacy policy and other matters related to the processing of the personal information and shall ensure the relevant rights of the Data Subject such as the right to access to the personal information, etc. Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work)

communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	(1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. <Amended Jul. 24, 2015> (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. Article 36 (Rectification or Deletion of Personal information) (1) The Data Subjects, who have accessed their own personal information pursuant to Article 35, may demand the correction or deletion of such personal information to the Personal information Controller; provided, however, that the deletion is not allowed where the said personal information is listed as subject to collection by other laws and regulations. (2) Upon receiving a demand from a Data Subject pursuant to paragraph (1), the Personal information Controller shall, without delay, review the personal information in question, and take necessary measures to correct or delete as demanded by the said Data Subject unless specific procedures are stipulated by other laws and regulations. Then the Personal information Controller shall notify the relevant Data Subject of the result.

		(3) The Personal information Controller shall take measures to preclude the possibility of restoring or recovering deleted personal information in case of deletion pursuant to paragraph (2). (4) When a request of a Data Subject applies to the proviso of paragraph (1), the Personal information Controller shall, without delay, notify the relevant Data Subjects of its content. (5) The Personal information Controller, while investigating the personal information in question pursuant to paragraph (2) may, if necessary, demand the evidence necessary to confirm the correction and deletion of the personal information to the relevant Data Subjects. (6) Necessary matters for the method and procedure for a demanded rectification and deletion, notification pursuant to paragraphs (1), (2) and (4) shall be followed as stipulated by presidential decree.
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was	Article 3 (Personal information Protection Principles) (3) The Personal information Controller shall ensure that the personal information is accurate, complete and up to date to the extent necessary to attain the purpose of processing the personal information. (5) The Personal information Controller shall disclose the privacy policy and other matters related to the processing of the personal information and shall ensure the relevant rights of the Data Subject such as the right to access to the personal information, etc. Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee

	disclosed, are required for compliance with this principle.	properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. Article 36 (Rectification or Deletion of Personal information) (1) The Data Subjects, who have accessed their own personal information pursuant to Article 35, may demand the correction or deletion of such personal information to the Personal information Controller; provided, however, that the deletion is not allowed where the said personal information is listed as subject to collection by other laws and regulations. (2) Upon receiving a demand from a Data Subject pursuant to paragraph (1), the Personal information Controller shall, without delay, review the personal information in question, and take necessary measures to correct or delete as demanded by the said Data Subject unless specific procedures are stipulated by other laws and regulations. Then the Personal information Controller shall notify the relevant Data Subject of the result. (3) The Personal information Controller shall take measures to preclude the possibility of restoring or recovering deleted personal information in case of deletion pursuant to paragraph (2). (4) When a request of a Data Subject applies to the proviso of paragraph (1), the Personal information Controller shall, without delay, notify the relevant Data Subjects of its content. (5) The Personal information Controller, while investigating the personal information in question pursuant to paragraph (2) may, if necessary, demand the evidence necessary to confirm the correction and deletion of the personal information to the relevant Data Subjects. (6) Necessary matters for the method and procedure for a demanded rectification and deletion, notification pursuant to paragraphs (1), (2) and (4) shall be followed as stipulated by presidential decree.
25. Do you require personal information	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the	Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work)

processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	(1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. (7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee.

Security Safeguards

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss,unauthorized access or disclosure, or other misuses*

Question (to be answered by the Applicant)	Assessment Criteria (to be verified by the Accountability Agent)	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
26. Have you implemented an information security policy?	Where the Applicant answers YES, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 59 (Prohibited Activities) No one who processes or had processed personal information shall engage in any of the following: 1. Obtain personal information or obtain the consent to personal information processing in a fraudulent, improper or unfair manner; 2. Reveal personal information obtained in the course of business, or provide it without rightful authority to another's use; or 3. Damage, lose, fabricate, forge or leak anyone's personal information without legal authority or beyond proper authority. Article 60 (Confidentiality, etc.) Any person who is or had been engaged in such business as stated in the following subparagraphs shall not reveal confidential information acquired while performing his/her duties to any other person, nor use such confidential information for any purpose other than the initial one; provided, however, that the same does not apply where specific provisions are stipulated in other Acts: 1. Any work of the Personal Information Protection Commission under Article 8; 2. Privacy impact assessment work under Article 33; and 3. Any dispute mediation handled by the Dispute Mediation Committee under Article 40. ENFORCEMENT DECREE

		Article 30 (Safety Measures of Personal Information) (1) The Personal information Controller shall take measures to ensure the safety of each of the following subparagraphs pursuant to Article 29 of the Act: 1. To set up and implement the internal management plan for the safe processing of personal information; 2. To control access to the personal information and restrict the authority to access hereto; 3. To adopt such encryption technology as to store and transmit the personal information in safety and other measures equivalent hereto; 4. To retain log-in records in order to respond data breach incidents and to take measures to prevent the forgery and falsification hereof; 5. To install and upgrade security programs to protect personal information; 6. To take such physical measures as storage to keep personal information in safety or locking system; or (2) The PIPC may provide such necessary assistance as building up the system with which the Personal information Controller may secure the safety measures subject to paragraph (1). (3) The PIPC shall make and notify the detailed standards regarding safety measures subject to paragraph (1).
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (eg password protections) Encryption • Boundary protection (eg firewalls, intrusion detection)	Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 59 (Prohibited Activities) No one who processes or had processed personal information shall engage in any of the following: 1. Obtain personal information or obtain the consent to personal information processing in a fraudulent, improper or unfair manner; 2. Reveal personal information obtained in the course of business, or provide it without rightful authority to another's use; or 3. Damage, lose, fabricate, forge or leak anyone's personal information without legal authority or beyond proper authority.

	Audit logging • Monitoring (eg external and internal audits, vulnerability scans) • Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information.	Article 60 (Confidentiality, etc.) Any person who is or had been engaged in such business as stated in the following subparagraphs shall not reveal confidential information acquired while performing his/her duties to any other person, nor use such confidential information for any purpose other than the initial one; provided, however, that the same does not apply where specific provisions are stipulated in other Acts: 1. Any work of the Personal Information Protection Commission under Article 8; 2. Privacy impact assessment work under Article 33; and 3. Any dispute mediation handled by the Dispute Mediation Committee under Article 40. Article 34 (Personal information Breach Notification, etc.) (1) The Personal information Controller shall notify the relevant Data Subjects without delay of the fact in the following subparagraphs when it becomes aware of the leakage of any personal information: 1. Items of personal information that had been leaked; 2. When and how the personal information was leaked; 3. Any measures that Data Subject may take in order to minimize probable damage that may break out due to leakage of personal information ; 4. Countermeasures of the Personal information Controller and remedial procedures; and 5. Help desk of the Personal information Controller and contact points for Data Subjects to report damages incurred due to the leakage of the personal information. (2) The Personal information Controller shall prepare countermeasures to minimize damage in case of any personal information leakage, and take necessary measures. (3) In case where a large scale of data breach above the level stipulated by presidential decree takes place, the Personal information Controller shall, without delay, report the notification stated in paragraph (1) and the result of measures stated in paragraph (2) to the PIPCand to such specific institution as stipulated by presidential decree. In such case, the PIPCand such specific institution as stipulated by presidential decree may provide technical assistance for the prevention and recovery of further damage, etc. (4) Necessary matters in relation to the time, method and procedure of the data breach notification pursuant to paragraph (1) shall be stipulated by presidential decree. ENFORCEMENT DECREE

	The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has NO physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	Article 30 (Safety Measures of Personal Information) (1) The Personal information Controller shall take measures to ensure the safety of each of the following subparagraphs pursuant to Article 29 of the Act: 1. To set up and implement the internal management plan for the safe processing of personal information; 2. To control access to the personal information and restrict the authority to access hereto; 3. To adopt such encryption technology as to store and transmit the personal information in safety and other measures equivalent hereto; 4. To retain log-in records in order to respond data breach incidents and to take measures to prevent the forgery and falsification hereof; 5. To install and upgrade security programs to protect personal information; 6. To take such physical measures as storage to keep personal information in safety or locking system; or (2) The PIPC may provide such necessary assistance as building up the system with which the Personal information Controller may secure the safety measures subject to paragraph (1). (3) The PIPC shall make and notify the detailed standards regarding safety measures subject to paragraph (1).
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information,	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative,	Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 23 (Limitation to Processing Sensitive Data) (2) In case the Personal information Controller processes the sensitive information pursuant to each subparagraph of paragraph (1), the Personal information Controller shall take the necessary measures to

and the context in which it is held.	technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	ensure the safety of the personal information including encryption, pursuant to Article 29, so that such sensitive data may not be lost, stolen, leaked, forged, altered or damaged. Article 24 (Limitation to Processing Unique Identifier) (3) In case the Personal information Controller processes the unique identifiers pursuant to each subparagraph of paragraph (1), the Personal information Controller shall take the necessary measures to ensure the safety of the personal information including encryption, as stipulated by presidential decree, so that such unique identifiers may not be lost, stolen, leaked, forged, altered or damaged. Article 24-2 (Limitation to Processing Resident Registration Numbers) (1) Notwithstanding Article 24(1), the Personal information Controller shall not, except for cases enumerated in the following subparagraphs, process the resident registration number: 1. Where laws and regulations require or permit processing of the resident registration number in a concrete manner; 2. Where it is deemed explicitly necessary for the impending protection of life, body and property of the Data Subject or a third person; or 3. Where it is inevitably necessary to process the resident registration number pursuant to an Order of the PIPC and provided that either subparagraphs 1 or 2 is satisfied. (2) Notwithstanding Article 24(3), the Personal information Controller shall preserve the resident registration numbers in safety by means of encryption so that they may not be lost, stolen, leaked, forged, fabricated or damaged. In such case, any necessary matters regarding the scope of encryption objects and encryption timing by object, etc. shall be

		stipulated by presidential decree in consideration of the volume of data processing and data breach impact, etc. (3) The Personal information Controller shall provide Data Subjects with effective methods to sign up without using the resident registration number at the stage of being admitted to membership via a website while processing the resident registration number pursuant to each subparagraph of paragraph 1. PERSONAL INFORMATION SAFEGUARD AND SECURITY STANDARD Article 1 (Purpose) The purpose of this Standard is to provide for detailed standards to secure safety so that personal information may not be lost, stolen, leaked, forged, altered or damaged when the Personal information Controller processes personal information pursuant to Articles 24(3) and 29 of the Personal Information Protection Act (hereinafter referred to as the “Act”) and Articles 21 and 30 of the Enforcement Decree of the same Act (hereinafter referred to as the “Decree”).

29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of	Article 28 (Supervision of the Personal information Manager) (1) The Personal information Controller shall see to it that the persons in charge of processing personal information, including employees, dispatched workers, part-timers, etc. are appropriately controlled and supervised by a designated manager (hereinafter the "Personal information Manager") in order to ensure that personal information is properly managed. (2) The Personal information Controller shall provide an appropriate educational program to the Personal information Manager on a regular basis to ensure appropriate handling thereof.

	such procedures are required for compliance with this principle.	
30. 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: 30. a) Employee training and management or other safeguards? 30. b) Information systems and	Where the Applicant answers YES (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers NO (to questions 30.a to 30.d), the Accountability Agent must inform	Article 28 (Supervision of the Personal information Manager) (1) The Personal information Controller shall see to it that the persons in charge of processing personal information, including employees, dispatched workers, part-timers, etc. are appropriately controlled and supervised by a designated manager (hereinafter the "Personal information Manager") in order to ensure that personal information is properly managed. (2) The Personal information Controller shall provide an appropriate educational program to the Personal information Manager on a regular basis to ensure appropriate handling thereof. Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 23 (Limitation to Processing Sensitive Data) (2) In case the Personal information Controller processes the sensitive data pursuant to each subparagraph of paragraph (1), the Personal information Controller shall take the necessary measures to ensure the

management, including network and software design, as well as information processing, storage, transmission, and disposal? 30. c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30. d) Physical security?	the Applicant that the existence of safeguards on each category is required for compliance with this principle.	safety of the personal information including encryption, pursuant to Article 29, so that such sensitive data may not be lost, stolen, leaked, forged, altered or damaged Article 24 (Limitation to Processing Unique Identifier) (3) In case the Personal information Controller processes the unique identifiers pursuant to each subparagraph of paragraph (1), the Personal information Controller shall take the necessary measures to ensure the safety of the personal information including encryption, as stipulated by presidential decree, so that such unique identifiers may not be lost, stolen, leaked, forged, altered or damaged. PERSONAL INFORMATION SAFEGUARD AND SECURITY STANDARD Article 1 (Purpose) The purpose of this Standard is to provide for detailed standards to secure safety so that personal information may not be lost, stolen, leaked, forged, altered or damaged when the Personal information Controller processes personal information pursuant to Articles 24(3) and 29 of the Personal Information Protection Act (hereinafter referred to as the "Act") and Articles 21 and 30 of the Enforcement Decree of the same Act (hereinafter referred to as the "Decree").
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers YES, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. ENFORCEMENT DECREE Article 30 (Safety Measures of Personal Information) (1) The Personal information Controller shall take measures to ensure the safety of each of the following subparagraphs pursuant to Article 29 of the Act: 1. To set up and implement the internal management plan for the safe processing of personal information; 2. To control access to the personal information and restrict the authority to access hereto;

		3. To adopt such encryption technology as to store and transmit the personal information in safety and other measures equivalent hereto; 4. To retain log-in records in order to respond data breach incidents and to take measures to prevent the forgery and falsification hereof; 5. To install and upgrade security programs to protect personal information; 6. To take such physical measures as storage to keep personal information in safety or locking system; or
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 31 (Designation of the Privacy Officer) (1) The Personal information Controller shall designate the Privacy Officer who comprehensively takes charge of the processing of the personal information (4) The Privacy Officer shall, upon becoming aware of any violation of this Act and other relevant laws and regulations in relation to personal information protection, immediately take corrective measures, and shall, if necessary, report such corrective measures to the head of the business entity or institution as well as any relevant outside organizations.
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify	Article 32-2 (Certification of Personal information Protection) (1) The PIPCmay certify whether the data processing and other personal information protection related action of the Personal information Controller abide by this Act, etc. (2) The certification pursuant to paragraph (1) shall be effective for three years. (3) The PIPCmay withdraw the certification pursuant to paragraph (1) as stipulated by presidential decree if any of the following subparagraphs applies; provided, 1. Personal information protection has been certified fraudulently or by other unjust means; 2. Ex post facto management under paragraph (4) has been denied or obstructed; 3. The certification criteria under paragraph (8) have not been satisfied; or 4. Violation of laws related to the protection of personal information in a serious manner.

	whether recommendations made in the audits are implemented.	(4) The PIPCshall conduct ex post facto management more than once a year to maintain the effectiveness of the certification of personal information protection. (5) The PIPCmay authorize a specialized institution stipulated by presidential decree to conduct certification subject to paragraph (1), withdrawal of such certification subject to paragraph (3), ex post facto management subject to paragraph (4), and management of the certification examiners subject to paragraph (7). (6) Any person who has obtained the certification subject to paragraph (1) may display or publicize the certification as stipulated by presidential decree. (7) The qualification, criteria of disqualification, etc. of the certification examiners who conduct the necessary certification examination subject to paragraph (1) shall be stipulated by presidential decree taking account of specialty, career and other necessary matters. (8) The criteria, method, and procedure of the certification, etc. pursuant to paragraph (1) and other necessary matters, including the determination on whether the management system of personal information, guarantee of Data Subject's rights and secured safeguards are in accordance with this Act, shall be stipulated by presidential decree. Article 33 (Privacy Impact Assessment) (1) Where the handling of personal information files applicable to the criteria stipulated by presidential decree may potentially infringe the personal information of Data Subjects, the head of the relevant public institution shall conduct an assessment (hereinafter the "Privacy Impact Assessment") for the analysis and improvement of such risk factors, and submit the results to the PIPC. In such a case, the head of the public institution shall request a Privacy Impact Assessment to the institutions (hereinafter the "PIA institution") designated by the PIPC. (2) The following subparagraphs shall be considered when conducting the Privacy Impact Assessment: 1. The number of personal information being processed; 2. Whether the personal information is provided to a third party or not; 3. The probability of the violation of any rights of Data Subjects and the degree of such risks; and 4. The other matters as stipulated by presidential decree.

		(3) The PIPCmay provide its opinion subject to the deliberation and resolution of the Commission upon receiving the PIA result as stated in paragraph (1). (4) The head of the public institution shall register the personal information files in accordance with Article 32(1), for which the Privacy Impact Assessment has been conducted pursuant to paragraph (1), with the PIA result attached thereto. (5) The PIPCshall prepare the necessary measures, such as fostering relevant specialists, and developing and disseminating PIA criteria, so as to properly activate the Privacy Impact Assessment. (6) Necessary matters in relation to the Privacy Impact Assessment, such as the driteria of designation and revocation of designation of the PIA institution, assessment criteria, method and procedure, etc. pursuant to paragraph (1) shall be stipulated by presidential decree. (7) A Privacy Impact Assessment conducted by the National Assembly, the Court, the Constitutional Court and the National Election Commission (including their agencies) shall be stipulated by the respective rules of the National Assembly, the Court, the Constitutional Court and the National Election Commission. (8) A Personal information Controller other than public institutions shall make best efforts to conduct the Privacy Impact Assessment if a violation of personal information is deemed highly probable.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction,	The Accountablity Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically	Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (2) A Personal information Controller who entrusts the processing of personal information to a third party pursuant to paragraph (1) (hereinafter the “entrustor”) shall disclose the persons who are or have been entrusted (hereinafter the “entrustee”) as well as the

use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	review and reassess its security measures to evaluate their relevance and effectiveness.	entrusted tasks related to the personal information to ensure that the Data Subjects may easily recognize it at any time in such a manner as stipulated by presidential decree. (3) The entrustor shall, in case of entrusting tasks related to public relations or the solicitation of goods or services, inform Data Subjects of the entrusted tasks and also the entrustee in such a manner as stipulated by presidential decree. The same shall apply when the entrusted tasks or entrustee has been changed. (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. (5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 34 (Personal information Breach Notification, etc.) (1) The Personal information Controller shall notify the relevant Data Subjects without delay of the fact in the following subparagraphs when it becomes aware of the leakage of any personal information: 1. Items of personal information that had been leaked; 2. When and how the personal information was leaked;

		3. Any measures that Data Subject may take in order to minimize probable damage that may break out due to leakage of personal information ; 4. Countermeasures of the Personal information Controller and remedial procedures; and 5. Help desk of the Personal information Controller and contact points for Data Subjects to report damages incurred due to the leakage of the personal information. (2) The Personal information Controller shall prepare countermeasures to minimize damage in case of any personal information leakage, and take necessary measures. (3) In case where a large scale of data breach above the level stipulated by presidential decree takes place, the Personal information Controller shall, without delay, report the notification stated in paragraph (1) and the result of measures stated in paragraph (2) to the PIPCand to such specific institution as stipulated by presidential decree. In such case, the PIPCand such specific institution as stipulated by presidential decree may provide technical assistance for the prevention and recovery of further damage, etc. (4) Necessary matters in relation to the time, method and procedure of the data breach notification pursuant to paragraph (1) shall be stipulated by presidential decree.

Access and Correction

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

Question	Assessment Criteria	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree.

	to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	Article 35 (Access to Personal information) (1) Data Subjects may demand access to their own personal information being processed by the Personal information Controller, to the relevant Personal information Controller. (2) Notwithstanding paragraph (1), when any Data Subject intends to request access to his/her own personal information to the public institution, the Data Subject may request directly to the said institution, or indirectly through the PIPCas stipulated by presidential decree. (3) The Personal information Controller shall, when it is requested access pursuant to paragraphs (1) and (2), ensure the Data Subjects have access to the relevant personal information within the period as stipulated by presidential decree. In such case, if there is any justifiable ground not to allow access within such period, the Personal information Controller may postpone access after notifying the relevant Data Subjects of the said reason. If the said reason expires, access is to be allowed without delay. (4) In case where any of the following subparagraphs is applicable, the Personal information Controller may restrict or deny access after notifying Data Subjects of the reason: *(omit)* (5) Necessary matters in relation to the method and procedure of request of access, access restriction, notification, etc. pursuant to paragraphs (1) through (4) shall be stipulated by presidential decree.
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) –	Where the Applicant answers YES the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable);

(e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37. a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37. b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37. c) Is information communicated in a reasonable manner that is generally	information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. Article 35 (Access to Personal information) (1) Data Subjects may demand access to their own personal information being processed by the Personal information Controller, to the relevant Personal information Controller. (2) Notwithstanding paragraph (1), when any Data Subject intends to request access to his/her own personal information to the public institution, the Data Subject may request directly to the said institution, or indirectly through the PIPCas stipulated by presidential decree. (3) The Personal information Controller shall, when it is requested access pursuant to paragraphs (1) and (2), ensure the Data Subjects have access to the relevant personal information within the period as stipulated by presidential decree. In such case, if there is any justifiable ground not to allow access within such period, the Personal information Controller may postpone access after notifying the relevant Data Subjects of the said reason. If the said reason expires, access is to be allowed without delay. (4) In case where any of the following subparagraphs is applicable, the Personal information Controller may restrict or deny access after notifying Data Subjects of the reason: *(omit)* (5) Necessary matters in relation to the method and procedure of request of access, access restriction, notification, etc. pursuant to paragraphs (1) through (4) shall be stipulated by presidential decree. Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public

understandable (in a legible format)? Please describe. 37. d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37. e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable); 4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree.
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your	Where the Applicant answers YES to questions 38.a, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide	Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 1. The purpose of processing the personal information; 2. The period for processing and retention of the personal information; 3. Provision of the personal information to a third party (if applicable);

applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a	the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers NO to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	4. Entrustment of processing the personal information (if applicable); 5. The rights and obligations of Data Subjects and methods to exercise such rights ; and 6. Other matters in relation to personal information processing as stipulated by presidential decree. Article 35 (Access to Personal information) (1) Data Subjects may demand access to their own personal information being processed by the Personal information Controller, to the relevant Personal information Controller. (2) Notwithstanding paragraph (1), when any Data Subject intends to request access to his/her own personal information to the public institution, the Data Subject may request directly to the said institution, or indirectly through the PIPCas stipulated by presidential decree. (3) The Personal information Controller shall, when it is requested access pursuant to paragraphs (1) and (2), ensure the Data Subjects have access to the relevant personal information within the period as stipulated by presidential decree. In such case, if there is any justifiable ground not to allow access within such period, the Personal information Controller may postpone access after notifying the relevant Data Subjects of the said reason. If the said reason expires, access is to be allowed without delay. (4) In case where any of the following subparagraphs is applicable, the Personal information Controller may restrict or deny access after notifying Data Subjects of the reason: *(omit)* (5) Necessary matters in relation to the method and procedure of request of access, access restriction, notification, etc. pursuant to paragraphs (1) through (4) shall be stipulated by presidential decree. Article 36 (Rectification or Deletion of Personal information) (1) The Data Subjects, who have accessed their own personal information pursuant to Article 35, may demand the correction or deletion of such personal information to the Personal information Controller;

reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?		provided, however, that the deletion is not allowed where the said personal information is listed as subject to collection by other laws and regulations. (2) Upon receiving a demand from a Data Subject pursuant to paragraph (1), the Personal information Controller shall, without delay, review the personal information in question, and take necessary measures to correct or delete as demanded by the said Data Subject unless specific procedures are stipulated by other laws and regulations. Then the Personal information Controller shall notify the relevant Data Subject of the result. (3) The Personal information Controller shall take measures to preclude the possibility of restoring or recovering deleted personal information in case of deletion pursuant to paragraph (2). (4) When a request of a Data Subject applies to the proviso of paragraph (1), the Personal information Controller shall, without delay, notify the relevant Data Subjects of its content. (5) The Personal information Controller, while investigating the personal information in question pursuant to paragraph (2) may, if necessary, demand the evidence necessary to confirm the correction and deletion of the personal information to the relevant Data Subjects. (6) Necessary matters for the method and procedure for a demanded rectification and deletion, notification pursuant to paragraphs (1), (2) and (4) shall be followed as stipulated by presidential decree. Article 37 (Suspension of Processing of Personal information, etc.) (1) Data Subjects may request the Personal information Controller to suspend the processing of their own personal information. In case the Personal information Controller is a public institution, the Data Subjects may request the suspension of processing of their personal information contained in the personal information files subject to being registered pursuant to Article 32. (2) Upon receiving a demand pursuant to paragraph (1), the Personal information Controller shall, without delay, suspend the processing of the said personal information in whole or in part as demanded by the Data Subject; provided, however, that, where any of the following subparagraphs is applicable, the Personal information Controller may reject the demand of the said Data Subject: 1. Where it is specifically stipulated by law or it is inevitably necessary to observe obligations under relevant laws and regulations;

		2. Where it may probably cause damage to the life or body of others, or improper violation of properties and benefits of others; 3. Where the public institution cannot carry out its work as prescribed by other laws without processing the personal information in question; or 4. Where it is difficult to fulfill a contract entered by and between the Personal information Controller and the Data Subject without processing the personal information and where the Data Subject fails to express explicitly the termination of the said contract. (3) The Personal information Controller shall, when rejecting the demand pursuant to the proviso of paragraph (2) notify the Data Subject of the reason without delay. (4) The Personal information Controller shall, without delay, take necessary measures including destruction of the relevant personal information when suspending the processing of personal information as demanded by a Data Subject. (5) Necessary matters in relation for the method and procedure of the demand or rejection of suspension of processing, notification, etc. pursuant to paragraphs (1) through (3) shall be stipulated by presidential decree.

Accountability

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question	Assessment Criteria	Enforceability (to be answered by the Economy) PERSONAL INFORMATION PROTECTION ACT
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) _____ • Contracts _____	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	Article 3 (Personal information Protection Principles) (1) The Personal information Controller shall explicitly specify the purpose of processing the personal information, and shall lawfully and fairly collect the minimum of such personal information to the extent necessary for such purposes. (2) The Personal information Controller shall appropriately process personal information to the extent necessary to attain the personal information processing purposes, and shall not use them for any other purposes. (3) The Personal information Controller shall ensure that the personal information is accurate, complete and up to date to the extent necessary to attain the purpose of processing the personal information. (4) The Personal information Controller shall manage the personal information in a safe manner according to personal information processing methods, types, etc. in consideration of the possibility that the rights of the Data Subject might be infringed upon and the degree of such risks.

• Compliance with applicable industry or sector laws and regulations ____ • Compliance with self-regulatory applicant code and/or rules ____ Other (describe) ____		(5) The Personal information Controller shall disclose the privacy policy and other matters related to the processing of the personal information and shall ensure the relevant rights of the Data Subject such as the right to access to the personal information, etc. (6) The Personal information Controller shall process personal information in a manner that minimizes infringement of the privacy of the Data Subject. (7) The Personal information Controller shall ensure that the personal information is processed anonymously, if possible. (8) The Personal information Controller shall make efforts to gain the trust of the Data Subjects by observing and carrying out such duties and responsibilities as stated in this Act and other related laws and regulations. Article 15 (Collection and Use of Personal information) (1) The Personal information Controller may collect personal information in any of the following cases, and use it within the scope of the collection purposes: 1. Where consent is obtained from Data Subjects; 2. Where special provisions exist in laws or it is inevitably necessary to observe obligations under the laws and regulations; 3. Where it is inevitably necessary for the public institution to carry out such work under its jurisdiction as prescribed by laws and regulations, etc.; 4. Where it is necessary so as to enter into and perform a contract with Data Subjects; 5. Where it is deemed explicitly necessary for the protection and, from impending danger, of the life, body or economic profits of the Data Subject or a third party in case the Data Subject or his/her legal representative is not in a position to express intention, or when prior consent cannot be obtained owing to unknown addresses; or 6. Where it is necessary to attain the legitimate interests of the Personal information Controller, which is explicitly superior to that of Data Subjects. In such case, collecting of personal information is allowed only to the extent where substantial relation exists with the legitimate interests of the Personal information Controller and doing so does not exceed a reasonable scope. (2) The Personal information Controller shall

		inform Data Subjects of the following when obtaining consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The purpose of collection and use of the personal information; 2. Items of personal information to be collected; 3. The use and retention period of the personal information; and 4. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. Article 16 (Limitations to Collection of Personal information) (1) The Personal information Controller shall collect the minimum personal information necessary to attain the purpose in any case applicable to any subparagraph of Article 15(1). In such case, the burden of proof that the minimum personal information is collected shall be borne by the Personal information Controller. (2) The Personal information Controller may collect personal information only after clearly informing the Data Subject that he/she may refuse consent to the collection of other personal information other than the minimum necessary. (3) The Personal information Controller shall not refuse the provision of goods or services to the Data Subjects on the ground that the Data Subject did not consent to the collection of personal information exceeding the minimum requirement. Article 17 (Provision of Personal information) (1) The Personal information Controller may provide (or share, hereinafter the same applies) the personal information of Data Subjects to a third party in cases applicable to any of the following subparagraphs: 1. Where the consent of the Data Subject is obtained; or 2. Where personal information is provided within the scope of purposes for which personal information is collected under subparagraphs 2, 3 and 5 of Article 15(1); (2) The Personal information Controller shall inform Data Subjects of the following when it obtains consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The recipient of the personal information; 2. The purpose of use of the personal information of the said recipient; 3. Items of personal information to be provided; 4. The use and retention period of the said recipient; and

		5. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3). (5) When a Personal information Controller provides personal information to a third party for a purpose other than the intended one in a case applicable to any of the subparagraphs of paragraph (2), the Personal information Controller shall request the recipient of the personal information to restrict the purpose and method of use and other necessary matters, or to prepare necessary measures to ensure the safety of the personal information. In such case, the person who is requested shall take necessary measures to ensure the safety of the personal information. Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information.

		(5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. (7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee. Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 34 (Personal information Breach Notification, etc.) (1) The Personal information Controller shall notify the relevant Data Subjects without delay of the fact in the following subparagraphs when it becomes aware of the leakage of any personal information: 1. Items of personal information that had been leaked; 2. When and how the personal information was leaked; 3. Any measures that Data Subject may take in order to minimize probable damage that may break out due to leakage of personal information ; 4. Countermeasures of the Personal information Controller and remedial procedures; and 5. Help desk of the Personal information Controller and contact points for Data Subjects to report damages incurred due to the leakage of the personal information. (2) The Personal information Controller shall prepare countermeasures to minimize damage in case of any personal information leakage, and take necessary measures.

		(3) In case where a large scale of data breach above the level stipulated by presidential decree takes place, the Personal information Controller shall, without delay, report the notification stated in paragraph (1) and the result of measures stated in paragraph (2) to the PIPCand to such specific institution as stipulated by presidential decree. In such case, the PIPCand such specific institution as stipulated by presidential decree may provide technical assistance for the prevention and recovery of further damage, etc. (4) Necessary matters in relation to the time, method and procedure of the data breach notification pursuant to paragraph (1) shall be stipulated by presidential decree.
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that designation of such an	Article 31 (Designation of the Privacy Officer) (1) The Personal information Controller shall designate the Privacy Officer who comprehensively takes charge of the processing of the personal information (2) The Privacy Officer shall carry out the tasks enumerated in the following subparagraphs: 1. Establishment and implementation of the personal information protection plan; 2. Conducting of inspections of the actual state and practices of the processing of personal information on a regular basis , and improvement of shortcomings; 3. Handling of complaints and compensation for damages incurred in relation to the processing of personal information; 4. Setting up of the required internal control system to prevent the leak, or abuse and misuse, of the personal information; 5. Establishment and implementation of the personal information protection education program; 6. Protection, control and management of the personal information files; and 7. Other functions for the appropriate processing of personal information as stipulated by presidential decree. (3) In carrying out the functions as enumerated in each subparagraph of paragraph (2), the Privacy Officer may inspect the system and status of the processing of personal information at any time, if necessary, and request a report thereof from the relevant parties. (4) The Privacy Officer shall, upon becoming aware of any violation of this Act and other relevant laws and regulations in relation to personal information protection, immediately

	employee(s) is required for compliance with this principle.	take corrective measures, and shall, if necessary, report such corrective measures to the head of the business entity or institution as well as any relevant outside organizations. (5) The Personal information Controller shall not have the Privacy Officer give or take disadvantages pertaining to personal information without any justifiable ground while conducting the tasks as stated in the subparagraphs of paragraph (2). (6) The requirements to be designated as a Privacy Officer, the tasks of the Privacy Officer, qualifications and other necessary matters shall be stipulated by presidential decree.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify).	Article 31 (Designation of the Privacy Officer) (2) The Privacy Officer shall carry out the tasks enumerated in the following subparagraphs: 3. Handling of complaints and compensation for damages incurred in relation to the processing of personal information; Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 6. Other matters in relation to personal information processing as stipulated by presidential decree. Article 39 (Liability for Damages) (1) A Data Subject, suffering damages caused by a violation of this Act of Personal information Controller, may claim damages against the Personal information Controller. In such case, the said Personal information Controller may not be released from the liability for damages if he/she fails to prove non-existence of its wrongful intent or negligence. 3) The court may order compensation not exceeding three times the actual damage suffered by the Data Subject due to loss, theft, leak, forgery, fabrication or damage of personal information, caused by wrongful intent or gross negligence of the Personal information Controller; provided, however, that this shall not apply to a Personal information Controller

	Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	who has proved that such act causing damages was not due to wrongful intent or gross negligence. (4) The court shall, in assessing compensation pursuant to paragraph (3), take into account the matters stated by the following subparagraphs: 1. Wrongful intent or degree of perception of the likelihood of the expected damage or of the likelihood of losses; 2. The amount of damage caused by violations; 3. Economic benefit gained by the Personal information Controller caused by the act of violation; 4. The criminal fine and penalty surcharge to be levied subject to violations; 5. The duration, velocity, etc. of the violations; 6. The financial condition of the Personal information Controller; 7. The efforts to retrieve the affected personal information exerted by the Personal information Controller after the loss, theft and leak of personal information; and 8. The efforts to remedy the damage suffered by a Data Subject exerted by the Personal information Controller Article 39-2 (Claim for Statutory Damages) (1) Notwithstanding Article 39(1), the Data Subject, if having suffered damage as a result of loss, theft, leak, forgery, fabrication or damage of personal information, caused by wrongful intent or negligence of a Personal information Controller, may claim a considerable amount of damages to the extent not exceeding three million won. In such case, the said Personal information Controller may not be released from the liability for damages if he/she fails to prove non-existence of wrongful intent or negligence. (2) In case of claims subject to paragraph (1), the court may assess a reasonable amount of compensation to the extent stated by paragraph (1) after taking into account all arguments in the proceedings and the examination of the evidence. (3) The Data Subject who has claimed damages pursuant to Article 39 may change such claim to a claim subject to paragraph (1) until the closing of the fact-finding proceedings.

42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	Article 31 (Designation of the Privacy Officer) (2) The Privacy Officer shall carry out the tasks enumerated in the following subparagraphs: 3. Handling of complaints and compensation for damages incurred in relation to the processing of personal information; Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 6. Other matters in relation to personal information processing as stipulated by presidential decree. Article 39 (Liability for Damages) (1) A Data Subject, suffering damages caused by a violation of this Act of Personal information Controller, may claim damages against the Personal information Controller. In such case, the said Personal information Controller may not be released from the liability for damages if he/she fails to prove non-existence of its wrongful intent or negligence. Article 39-2 (Claim for Statutory Damages) (1) Notwithstanding Article 39(1), the Data Subject, if having suffered damage as a result of loss, theft, leak, forgery, fabrication or damage of personal information, caused by wrongful intent or negligence of a Personal information Controller, may claim a considerable amount of damages to the extent not exceeding three million won. In such case, the said Personal information Controller may not be released from the liability for damages if he/she fails to prove non-existence of wrongful intent or negligence.
43. If YES, does this response include an explanation of	The Accountability Agent must verify that the Applicant indicates	Article 31 (Designation of the Privacy Officer) (2) The Privacy Officer shall carry out the tasks enumerated in the following subparagraphs:

remedial action relating to their complaint? Describe.	what remedial action is considered.	3. Handling of complaints and compensation for damages incurred in relation to the processing of personal information; Article 30 (Establishment and Disclosure of Privacy Policy) (1) The Personal information Controller shall establish a personal information processing policy including the particulars in the following subparagraphs (hereinafter the "Privacy Policy"). In such case, the public institutions shall set up the Privacy Policy regarding the personal information files subject to be registered pursuant to Article 32: 6. Other matters in relation to personal information processing as stipulated by presidential decree. Article 39 (Liability for Damages) (1) A Data Subject, suffering damages caused by a violation of this Act of Personal information Controller, may claim damages against the Personal information Controller. In such case, the said Personal information Controller may not be released from the liability for damages if he/she fails to prove non-existence of its wrongful intent or negligence. Article 39-2 (Claim for Statutory Damages) (1) Notwithstanding Article 39(1), the Data Subject, if having suffered damage as a result of loss, theft, leak, forgery, fabrication or damage of personal information, caused by wrongful intent or negligence of a Personal information Controller, may claim a considerable amount of damages to the extent not exceeding three million won. In such case, the said Personal information Controller may not be released from the liability for damages if he/she fails to prove non-existence of wrongful intent or negligence.
44. Do you have procedures in place for training employees with respect to your privacy policies and	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures,	Article 28 (Supervision of the Personal information Manager) (1) The Personal information Controller shall see to it that the persons in charge of processing personal information, includng employees,. dispatched workers, part-timers, etc. are appropriately controlled and supervissed by a designated manager (hereinafter the "Personal information Manager") in order to ensure that personal information is properly managed.

procedures, including how to respond to privacy-related complaints? If YES, describe.	including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	(2) The Personal information Controller shall provide an appropriate educational program to the Personal information Manager on a regular basis to ensure appropriate handling thereof. Article 31 (Designation of the Privacy Officer) (2) The Privacy Officer shall carry out the tasks enumerated in the following subparagraphs: 5. Establishment and implementation of the personal information protection education program;
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3). (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, the Personal information Controller may use personal information for a purpose other than the intended one, or provide it to a third party, unless it likely infringes upon unfairly the interests of Data Subjects or a third party; provided, however, that subparagraphs 5 through 9 are applicable only to public institutions. 2. Where special provisions exist in laws; 7. Where it is necessary to investigate crimes, and launch and sustain a prosecution; 8. Where it is necessary for the court to perform its judicial affairs; or 9. Where it is necessary to execute a punishment, take custody, or for protective disposition. (4) When a public institution uses personal information for a purpose other than the intended one, or provides it to a third party under subparagraphs 2 through 6, 8 and 9, the public institution shall post the legal grounds for such use or provision, purpose and scope, and other necessary matters in its own publication and/or its own website as prescribed by the Ordinance of the PIPC.

46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-regulatory applicant code and/or rules _____ • Other (describe) _____	Where the Applicant answers YES, the Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. <Amended Jul. 24, 2015> (5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. (7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee.

47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____ • Follow instructions provided by you relating to the manner in which your personal information must be handled? _____	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. <Amended Jul. 24, 2015> (5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. (7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee. Article 29 (Duty of Security Measures) The Personal information Controller shall take technical, managerial and physical measures such as establishment of internal management plan and preservation of log-on records, etc. necessary to ensure security as stipulated by presidential decree so as to prevent personal information from being lost, stolen, leaked, forged, fabricated or damaged. Article 34 (Personal information Breach Notification, etc.) (1) The Personal information Controller shall notify the relevant Data Subjects without delay of the fact in the following subparagraphs when it becomes aware of the leakage of any personal information:

• Impose restrictions on subcontracting unless with your consent? _____ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ • Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? • Other (describe) _____		1. Items of personal information that had been leaked; 2. When and how the personal information was leaked; 3. Any measures that Data Subject may take in order to minimize probable damage that may break out due to leakage of personal information ; 4. Countermeasures of the Personal information Controller and remedial procedures; and 5. Help desk of the Personal information Controller and contact points for Data Subjects to report damages incurred due to the leakage of the personal information. (2) The Personal information Controller shall prepare countermeasures to minimize damage in case of any personal information leakage, and take necessary measures. (3) In case where a large scale of data breach above the level stipulated by presidential decree takes place, the Personal information Controller shall, without delay, report the notification stated in paragraph (1) and the result of measures stated in paragraph (2) to the PIPC and to such specific institution as stipulated by presidential decree. In such case, PIPC and such specific institution as stipulated by presidential decree may provide technical assistance for the prevention and recovery of further damage, etc. (4) Necessary matters in relation to the time, method and procedure of the data breach notification pursuant to paragraph (1) shall be stipulated by presidential decree.
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or	The Accountability Agent must verify the existence of such self-assessments.	Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the

agreements/contracts? If YES, describe below.		entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. <Amended Jul. 24, 2015> (5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor. (7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers YES, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers NO, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	Article 26 (Limitation to Processing Personal information Subsequent to Entrustment of Work) (1) The Personal information Controller shall, when entrusting the processing of personal information to a third party, shall implement and use paper-based formalities as stated in the following subparagraphs: 1. Prevention of processing personal information for any purposes other than those intended; 2. Technical and managerial safeguards of personal information; and 3. Other matters stipulated by presidential decree for the safe management of personal information (4) The entrustor shall instruct the entrustee to prevent the personal information of Data Subjects from being lost, stolen, leaked, forged, fabricated or damaged due to the entrustment of tasks and shall supervise the entrustee to ensure that the entrustee properly manages, protects and processes such personal information in accordance with methods stipulated by presidential decree, such as inspecting of processing the personal information. <Amended Jul. 24, 2015> (5) The entrustee shall not use personal information beyond the scope of the tasks entrusted by the Personal information Controller, nor provide such personal information to a third party. (6) When civil liability to pay compensation arises as an entrustee violates this Act in the course of processing personal information in connection with the entrusted tasks, the entrustee shall be deemed as an employee of the entrustor.

		(7) Articles 15 through 25, 27 through 31, 33 through 38 and 59 shall apply mutatis mutandis to the entrustee.
50. Do you disclose personal information to other recipient persons or organisations in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If YES, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	Article 17 (Provision of Personal information) (1) The Personal information Controller may provide (or share, hereinafter the same applies) the personal information of Data Subjects to a third party in cases applicable to any of the following subparagraphs: 1. Where the consent of the Data Subject is obtained; or 2. Where personal information is provided within the scope of purposes for which personal information is collected under subparagraphs 2, 3 and 5 of Article 15(1); (2) The Personal information Controller shall inform Data Subjects of the following when it obtains consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed: 1. The recipient of the personal information; 2. The purpose of use of the personal information of the said recipient; 3. Items of personal information to be provided; 4. The use and retention period of the said recipient; and 5. The fact that Data Subjects are entitled to refuse consent, and details of disadvantage, if any, due to refusal of consent. (3) When a Personal information Controller provides personal information to a third party located overseas, the Personal information Controller shall first inform the Data Subjects of any of the subparagraphs of paragraph (2), and obtain consent from them. The Personal information Controller shall not enter into a contract for the cross-border transfer of personal information in violation of this Act. Article 18 (Limitations to Out-of-Purpose Use and Provision of Personal information) (1) The Personal information Controller shall not use personal information beyond the scope stated in Article 15(1), and shall not provide it to a third party beyond the scope stated in Article 17(1) and (3). (5) When the personal information controller provides personal information to a third party for other purpose than the intended one in the case applicable to any of subparagraphs of paragraph (2), the personal information controller shall request the recipient of personal information to restrict the purpose and method of use and other necessary matters, or to prepare for necessary safeguards to ensure the safety of personal information. In this case,

		the person who is requested shall take necessary measures to ensure the safety of personal information. Article 19 (Limitations on the Use and Provision of Personal information on the Part of the Recipient) A person who receives personal information from a Personal information Controller shall not use such personal information for purposes other than the intended one, or shall not provide it to a third party except in cases applicable to any of the following subparagraphs: 1. Where separate consent is obtained from Data Subjects; or 2. Where special provisions exist in other laws,

◈ Please refer to the Sanction Provisions of the PIPA as below.

Article 34-2 (Imposition, etc. of Penalty Surcharge) (1) The PIPC may impose and collect penalty surcharges not exceeding 500 million won in cases where the Personal information Controller caused the loss, theft, leak, forgery, fabrication or damages of resident registration numbers; *provided, however*, that this shall not apply if and when the Personal information Controller has fully taken measures necessary to ensure the safety subject to Article 24(3) to prevent any loss, theft, leak, forgery, fabrication or damage of resident registration numbers.

(2) The PIPC shall take into consideration, when imposing penalty surcharges pursuant to paragraph (1), the following subparagraphs:
1. The degree of efforts being taken to perform the safety measures subject to Article 24(3);
2. The degree of loss, theft, leak, forgery, fabrication or destruction of resident registration numbers ;
3. Whether subsequent measures to prevent the spread of damage have been implemented.

(3) The PIPC shall collect an additional charge of up to 6% per annum of the unpaid penalty surcharge as stipulated by presidential decree for the period from the day following the expiration of the period of the penalty surcharge payment to the preceding day of payment of the penalty surcharge, in case the person subject to penalty surcharge payment pursuant to paragraph (1) fails to pay the penalty surcharge within the period of payment. In such case, the additional charge may be collected for up to but not exceeding 60 months.

(4) The PIPC shall, in case a person subject to the penalty surcharge payment pursuant to paragraph (1) fails to pay the sum of penalty surcharge within the period of payment, give a notice with the period of payment specified in it and, in case original and additional charges pursuant to paragraph (2) are not paid within the period of payment, collect penalty surcharges in a manner similar to collection of national taxes in arrears.

(5) Other matters necessary for the imposition and collection of penalty surcharges shall be stipulated by presidential decree.

Article 70 (Penalties) Any person found guilty of any of the conditions in the following subparagraphs shall be subject to imprisonment with prison labor for up to 10 years or fined up to 100 million won.
1. A person who modified or destroyed data subject to processing by a public institution for the purpose of interrupting the processing of such thereby causing suspension and/or paralysis of the business associated with the public institution.
2. A person who has obtained personal information processed by others by fraud or other unjust means or methods and provided it to a third party for profit or unjust purpose, and who has aided and abetted such unlawful activity.

Article 71 (Penalties) Any person found guilty of any of the conditions in the following subparagraphs shall be subject to imprisonment with prison labor for up to 5 years or fined up to 50 million won:

1. A person who has provided personal information to a third party without the consent of Data Subjects in violation of Article 17(1)i even though Article 17(1)ii does not apply, and knowingly received the said personal information;
2. A person who has used or provided to a third party personal information in violation of Articles 18(1) and (2), 19, 26(5) or 27(3), and knowingly received the said personal information for profit-making or unfair purposes;
3. A person who has processed sensitive data in violation of Article 23;
4. A person who has processed a unique identifier in violation of Article 24(1);
5. A person who has revealed, or provided to other persons without authority, personal information acquired from business in violation of Article 59ii, and knowingly received the said personal information for profit-making or unfair purposes; or
6. A person who has damaged, lost, fabricated, forged or leaked the personal information of others in violation of Article 59iii.

Article 72 (Penalties) Any person found guilty of any of the conditions in the following subparagraphs shall be subject to imprisonment with prison labor for up to 3 years or fined up to 30 million won:
1. A person who has arbitrarily operated image data processing devices for purposes other than the intended one, or directed the said devices toward different spots, or used sound recording functions in violation of Article 25(5)
2. A person who has got personal information or obtained the consent to personal information processing in a fraudulent or unfair manner, and a person who has knowingly received such personal information for profit-making or unfair purposes in violation of Article 59i; or
3. A person who has revealed confidential information acquired while performing his/her duties to another person, or used such secrets for purposes other than the intended one in violation of Article 60.

Article 73 (Penalties) Any person found guilty of any of the conditions in the following subparagraphs shall be subject to imprisonment with prison labor for up to 2 years or fined up to 10 million won:
1. A person who has failed to take necessary measures to ensure safety in violation of Articles 24(3), 25(6) or 29, and caused the personal information to be lost, stolen, leaked, forged, fabricated or damaged;
2. A person who has failed to take necessary measures to rectify or delete personal information in violation of Article 36(2), and continuously use, or provide the personal information to a third party; or
3. A person who has failed to suspend the processing of personal information in violation of Article 37(2), and continuously used or provide the personal information to a third party

Article 74 (Joint Penalties) (1) If the representative of a corporation or an agent, manager or other employee of a corporation or an individual has violated any provision of Article 70 with respect to the business of such corporation or individual, not only the actor but also the corporation or individual shall be subject to a punitive fine of up to 70 million won; provided, however, that the same shall not apply where such corporation or individual was not negligent in taking due care and supervisory duty to prevent the actor from the said violation.

(2) If the representative of a corporation or an agent, manager or other employee of a corporation or an individual violated any of the provisions from Articles 71 through 73 with respect to the business of such corporation or individual, not only the actor but also the corporation or individual shall be subject to a punitive fine prescribed in the relevant Article; provided, however, that the same shall not apply where such corporation or individual was not negligent in taking due care and supervisory duty to prevent the actor from the said violation.

Article 74-2 (Forfeiture, Additional Collection, etc.) Any money, goods or other benefits acquired by an offender in violation of Articles 70 through 73 in relation to such violations may be forfeited, or, if forfeiture is impossible, the value thereof may be collected. In such case, additional collection may be levied in conjunction with other penal provision.

Article 75 (Administrative Fine) (1) Any person found guilty of any of the conditions in the following subparagraphs shall be subject to a administrative fine of up to 50 million won:

1. A person who has collected personal information in violation of Article 15(1);
2. A person who has failed to obtain consent from a legal representative in violation of Article 22(5); or
3. A person who has installed and operated image data processing devices in violation of Article 25(2).

(2) Any person found guilty of any of the conditions in the following subparagraphs shall be subject to a administrative fine of up to 30 million won:

1. A person who has failed to inform Data Subjects of necessary data in violation of Articles 15(2), 17(2), 18(3) or 26(3);
2. A person who has refused the provision of goods or services to Data Subjects in violation of Articles 16(3) or 22(4);
3. A person who has failed to notify Data Subjects of the fact stated in the subparagraphs of Article 20(1) in violation of the same paragraph;
4. A person who has failed to destroy personal information in violation of Article 21(1);

4-2. A person who has processed the resident registration numbers in violation of Article 24-2(1);

4-3. A person who has failed to adopt encryption in violation of Article 24-2(2);

5. A person who has failed to provide Data Subjects with an alternative method that does not use their resident registration numbers in violation of Article 24-2(3);
6. A person who has failed to take necessary measures to ensure the safety of personal information in violation of Articles 24(3), 25(6) or 29;
7. A person who has installed and operated image data processing devices in violation of Article 25(1);

7-2. A person who has fraudulently marked and promoted a certification despite the failure of such certification in violation of Article 32-2(6);

8. A person who has failed to notify Data Subjects of the fact as per the subparagraphs of Article 34(1) in violation of the same paragraph;
9. A person who has failed to report the result of the notification in violation of Article 34(3);
10. A person who has restricted or denied access to personal information in violation of Article 35(3);
11. A person who has failed to take necessary measures to rectify or delete personal information in violation of Article 36(2);
12. A person who has failed to take necessary measures including destruction of personal information whose processing was suspended in violation of Article 37(4); or

13. A person who has failed to observe the corrective measures pursuant to Article 64(1).

(3) omit

(4) Any person found guilty of any of the conditions in the following subparagraphs shall be subject to a administrative fine of up to 10 million won:

1. A person who has failed to store and manage personal information separately in violation of Article 21(3);
2. A person who has obtained consent in violation of Article 22(1) through (3);
3. A person who has failed to take necessary measures including posting on a signboard in violation of Article 25(4);
4. A person who has failed to file required paper-based formalities during the entrustment tasks stated in the subparagraphs of Article 26(1) in violation of the same paragraph;
5. A person who has failed to disclose the entrustment tasks and the entrustee in violation of Article 26(2);
6. A person who has failed to notify Data Subjects of the transfer of personal information in violation of Article 27(1) and (2);
7. A person who has failed to establish, or disclose, the personal information processing policy in violation of Article 30(1) or (2);
8. A person who has failed to designate a Privacy Officer in violation of Article 31(1);
9. A person who has failed to provide Data Subjects with necessary data in violation of Articles 35(3) and (4), 36(2) and (4) or 37(3);
10. A person who has failed to furnish materials such as goods, documents, etc. pursuant to Article 63(1), or who submitted them in a fraudulent manner; or
11. A person who has rejected, obstructed or avoided the entry, inspection and examination of personal information pursuant to Article 63(2).

(5) The administrative fine pursuant to paragraphs (1) through (3) shall be imposed and collected by the PIPC and the heads of the relevant central administrative departments concerned as stipulated by presidential decree. In such case, the head of central administrative departments concerned shall impose and collect the fine for negligence from the Personal Information Controller in the field under its jurisdiction.