GLOBAL CROSS-BORDER PRIVACY RULES SYSTEM(CBPR)
ENFORCEMENT MAP

*The purpose of this document is to provide the baseline program requirements of the Global Cross-Border Privacy Rules (CBPR) System which are based on the Global CBPR Privacy Principles ("**Privacy Principles**")[1], and assist Global CBPR Forum-recognized Accountability Agents ("**Accountability Agents**") in reviewing an Applicant Organization's compliance with the Global CBPR System.*

These program requirements are replicated in the Global CBPR System Intake Questionnaire to help Applicant Organizations assess their compliance.

Accountability Agents are responsible for receiving an Applicant Organization's completed Intake Questionnaire and supporting documentation, verifying an Applicant Organization's compliance with the requirements of the Global CBPR System and, where appropriate, assisting the Applicant Organization in modifying its policies and practices to meet the requirements of the Global CBPR System. The Accountability Agent will certify those Applicant Organizations deemed to have met the minimum criteria for participation provided herein, and will be responsible for monitoring the Certified Organizations' compliance with the Global CBPR System based on these criteria.

[1] The Global CBPR Privacy Principles are described in the *Global CBPR Framework*, available at http://www.globalcbpr.org/documents/.

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. The list of acceptable Qualifications to the Provision of Notice is below.

Question	Assessment Criteria	Enforceability – Korea 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 Organization's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant Organization'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 Global CBPR Framework; • Is easy to find and accessible; • Applies to all personal information, whether collected online or offline; and • States an effective date of privacy statement publication.	**Article 30 (Establishment and Disclosure of Privacy Policy)** (1) A personal information controller shall establish a personal information processing policy including the following matters (hereinafter referred to as "Privacy Policy"). In such cases, public institutions shall establish the Privacy Policy for the personal information files to be registered pursuant to Article 32: *<Amended on Mar. 29, 2016; Feb. 4, 2020; Mar. 14, 2023>* 1. The purposes for which personal information is processed; 2. The period for processing and retaining personal information; 3. Provision of personal information to a third party (if applicable); 3-2. Procedures and methods for destroying personal information (if personal information shall be preserved according to the provison of Article 21 (1), this shall include the basis of preservation and particulars of personal information to be preserved);

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
	Where Applicant Organization answers **NO to question 1** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization that Notice as described herein is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	3-3. The possibility of disclosure of sensitive information and the method of selecting non-disclosure under Article 23 (3) (if applicable); 4. Entrusting personal information processing (if applicable); 4-2. Matters relating to processing, etc. of pseudonymized information under Articles 28-2 and 28-3 (if applicable); 5. The rights and obligations of data subjects and legal representatives, and how to exercise such rights; 6. Contact information, such as the name of a privacy officer designated under Article 31 or the name, telephone number, etc. of the department which performs the work related to personal information protection and handles related grievances; 7. Installation and operation of an automatic collection tool for personal information, including Internet access data files, and the denial thereof (if applicable); 8. Other matters prescribed by Presidential Decree regarding the processing of personal information. (2) Upon establishing or modifying the Privacy Policy, a personal information controller shall disclose the content so that data subjects may easily recognize it in such a way as prescribed by Presidential Decree.
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 Organization. • 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.	

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
	If **NO**, the Accountability Agent must inform the Applicant Organization that Notice as described herein is required for compliance with this Privacy Principle.	(3) Where there exist discrepancies between the Privacy Policy and the agreement executed by and between the personal information controller and data subjects, the terms that are beneficial to the data subjects shall prevail. (4) The Protection Commission may prepare the Privacy Policy Guidelines and encourage the personal information controllers to comply with such Guidelines. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020>*
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must notify the Applicant Organization that notice of the purposes for which personal information is collected is required and must be included in their privacy statement. Where the Applicant Organization 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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization notifies individuals that their personal information will or may be made available to third parties, **identifies the categories or specific third parties, and the**	

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
	purpose for which the personal information will or may be made available. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must notify the Applicant Organization that notice that personal information will be available to third parties is required and must be included in their privacy statement. Where the Applicant Organization 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 Organization's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization provides name, address and a **functional** e-mail address. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization that such disclosure of information is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization'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 Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization, that such information is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant Organization 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 Organization answers **NO** and does not identify an applicable Qualification listed below, the Accountability Agent must inform the Applicant Organization that providing information about access and correction, including the Applicant Organization's typical response times for access and correction requests, is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that the notice that personal information is being collected is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	**Article 15 (Collection and Use of Personal Information)** (1) A personal information controller may collect personal information in any of the following cases, and use it within the scope of the purpose of collection: *<Amended on Mar. 14, 2023>* 1. Where consent is obtained from a data subject; 2. Where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations; 3. Where it is unavoidable for a public institution's performance of work under its jurisdiction as prescribed by statutes or regulations, etc.; 4. Where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract; 5. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party; 6. Where it is necessary to attain the legitimate interests of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the legitimate
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 Organization's website, such as text on a website link from URL, attached documents, pop-up window, or other.	

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
	Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	interests of the personal information controller and does not go beyond a reasonable scope. 7. Where it is urgently necessary for the public safety and security, public health, etc. (2) A personal information controller shall inform a data subject of the following matters when it obtains consent under paragraph (1) 1. The same shall apply when any of the following is modified: 1. The purpose of the collection and use of personal information; 2. Particulars of personal information to be collected; 3. The period for retaining and using personal information; 4. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (3) A personal information controller may use personal information without the consent of a data subject within the scope reasonably related to the initial purpose of the collection as prescribed by Presidential Decree, in consideration whether disadvantages have been caused to the data subject and whether necessary measures to ensure safety such as encryption have been taken. *<Newly Inserted on Feb. 4, 2020>*

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
		Article 22 (Methods of Obtaining Consent) **...** (2) Where a personal information controller obtains the consent under paragraph (1) in writing (including electronic documents under Article 2, subparagraph 1 of the Framework Act on Electronic Documents and Transactions), the personal information controller shall clearly specify important matters prescribed by Presidential Decree such as the purpose of collection and use of personal information and the items of personal information to be collected and used, in the manner prescribed by Notification of the Protection Commission, so as to make such matters easy to be understood. *<Newly Inserted on Apr. 18, 2017; Jul. 26, 2017; Feb. 4, 2020>* (3) With respect to the personal information that can be processed without consent of the data subject, a personal information controller shall disclose the relevant items and legal basis for such processing under Article 30 (2) by separating such information from the personal information processed with consent of the data subject, or shall inform the data subject thereof by e-mail or any other means prescribed by Presidential Decree. In such cases, the burden of proof that personal information can be processed without consent shall be borne by the personal information controller. *<Amended on Mar. 29, 2016; Apr. 18, 2017; Mar. 14, 2023>* **...**

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must determine whether the applicable Qualification is justified.	**Article 17 (Provision of Personal Information)** (1) A personal information controller may provide (or share; hereinafter the same shall apply) the personal information of a data subject to a third party in any of the following cases: <*Amended on Feb. 4, 2020; Mar. 14, 2023*> 1. Where consent is obtained from the data subject; 2. Where the personal information is provided within the scope of purposes for which it is collected pursuant to Articles 15 (1) 2, 3, and 5 through 7. (2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose for which the recipient of personal information uses such information; 3. Particulars of personal information to be provided; 4. The period during which the recipient retains and uses personal information; 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (3) Deleted. <*Mar. 14, 2023*>

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
		(4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether measures necessary to secure safety, such as encryption, have been taken, etc. *<Newly Inserted on Feb. 4, 2020>* **Article 26 (Restriction on Personal Information Processing Subsequent to Entrustment of Work)** (1) A personal information controller shall, when entrusting the processing of personal information to a third party, do so in a document that states the following: *<Amended on Mar. 14, 2023>* 1. Prevention of personal information processing for other purposes than performing the entrusted work; 2. Technical and managerial safeguards of personal information; 3. Other matters prescribed by Presidential Decree to ensure safe management of personal information. (2) A personal information controller who entrusts the processing of personal information pursuant to paragraph (1) (hereinafter referred to as "person entrusting") shall disclose the details of the entrusted

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
		affairs and the entity that processes personal information (including a third party re-entrusted from a person entrusted with the processing of personal information; hereinafter referred to as "person entrusted") in the manner prescribed by Presidential Decree so as to be easily recognizable by data subjects at any time. <*Amended on Mar. 14, 2023*> (3) The person entrusting shall, in case of entrusting the promotion of goods or services, or soliciting of sales thereof, notify data subjects of the entrusted work and the person entrusted in the manners prescribed by Presidential Decree. The same shall apply where the entrusted work or the person entrusted has been changed. (4) The person entrusting shall educate the person entrusted so that personal information of data subjects may not be lost, stolen, divulged, forged, altered, or damaged owing to the outsourcing of work, and supervise how the person entrusted processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree. <*Amended on Jul. 24, 2015*> (5) An person entrusted shall not use any personal information beyond the scope of the work entrusted by the personal information controller, nor provide personal information to a third party. (6) A person entrusted shall, when he or she intends to re-entrust the processing of entrusted personal information to a third party, obtain consent from the person entrusting. <*Newly Inserted on Mar. 14,*

Question	Assessment Criteria	Enforceability – Korea Personal Information Protection Act
		2023> (7) With respect to liability for damages arising out of the processing of personal information entrusted to an person entrusted in violation of this Act, the person entrusted shall be deemed an employee of the personal information controller. <*Amended on Mar. 14, 2023*> (8) Articles 15 through 18, 21, 22, 22-2, 23, 24, 24-2, 25, 25-2, 27, 28, 28-2 through 28-5, 28-7 through 28-11, 29, 30, 30-2, 31, 33, 34, 34-2, 35, 35-2, 36, 37, 37-2, 38, 59, 63, 63-2, and 64-2 shall apply mutatis mutandis to outsourcees. In such cases, "personal information controller" shall be construed as "person entrusted". <*Amended on Mar. 14, 2023*>

Qualifications to the Provision of Notice

The following are situations in which the application at the time of collection of the Global CBPR Notice Principle may not be necessary or practical.

i. **Obviousness:** Personal information controllers do not need to provide notice of the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information (e.g., if an individual gives his or her business card to another individual in the context of a business relationship, the individual would not expect that notice would be provided regarding the collection and normal use of that information).

ii. **Collection of Publicly-Available Information**: Personal information controllers do not need to provide notice regarding the collection and use of publicly available information.

iii. **Technological Impracticability**: Personal information controllers do not need to provide notice at or before the time of collection in those cases where electronic technology automatically collects information when a prospective customer initiates contact (e.g., through the use of cookies). However, the notice should be provided to the individuals as soon after as is practicable.

iv. **Disclosure to a government institution which has made a request for the information with lawful authority:** Personal information controllers do not need to provide notice of disclosure to law enforcement agencies for investigation purposes where the provision of such notice to the individual will likely prejudice the investigation.

v. **Disclosure to a third party pursuant to a lawful form of process:** Personal information controllers do not need to provide notice of disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vi. **Third-Party Receipt**: Where personal information is received from a third party, the recipient personal information controller does not need to provide notice to the individuals at or before the time of collection of the information.

vii. **For legitimate investigation purposes:** When providing notice would compromise the availability or accuracy of the information and the collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. **Action in the event of an emergency**: Personal information controllers do not need to provide notice in emergency situations that threaten the life, health or security of an individual.

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	Assessment Criteria	Enforceability
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 Organization indicates from whom they obtain personal information. Where the Applicant Organization answers **YES to any of these sub-parts**, the Accountability Agent must verify the Applicant Organization'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 Organization that it has incorrectly completed the questionnaire.	**Article 15 (Collection and Use of Personal Information)** (1) A personal information controller may collect personal information in any of the following cases, and use it within the scope of the purpose of collection: *<Amended on Mar. 14, 2023>* 1. Where consent is obtained from a data subject; 2. Where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations; 3. Where it is unavoidable for a public institution's performance of work under its jurisdiction as prescribed by statutes or regulations, etc.; 4. Where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract; 5. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party;

Question	Assessment Criteria	Enforceability
		6. Where it is necessary to attain the legitimate interests of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the legitimate interests of the personal information controller and does not go beyond a reasonable scope. 7. Where it is urgently necessary for the public safety and security, public health, etc. (2) A personal information controller shall inform a data subject of the following matters when it obtains consent under paragraph (1) 1. The same shall apply when any of the following is modified: 1. The purpose of the collection and use of personal information; 2. Particulars of personal information to be collected; 3. The period for retaining and using personal information; 4. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (3) A personal information controller may use personal information without the consent of a data subject within the scope reasonably related to the initial purpose of the collection as prescribed by Presidential Decree, in consideration whether disadvantages have been caused to the data subject

Question	Assessment Criteria	Enforceability
		and whether necessary measures to ensure safety such as encryption have been taken. <*Newly Inserted on Feb. 4, 2020*> **Article 20 (Notification of Sources of Personal Information Collected from Other Than Data Subjects)** (1) When a personal information controller processes personal information collected from sources other than data subjects, the personal information controller shall immediately notify the data subject of the following matters at the request of such data subject: <*Amended on Mar. 14, 2023*> 1. The source of collected personal information; 2. The purpose of processing personal information; 3. The fact that the data subject is entitled to request suspension of processing of personal information or to withdraw consent, as prescribed in Article 37. (2) Notwithstanding paragraph (1), when a personal information controller satisfying the criteria prescribed by Presidential Decree taking into account the types and amount of processed personal information, number of employees, amount of sales, etc., collects personal information from third parties and processes the same pursuant to Article 17 (1) 1, the personal information controller shall notify the data subject of the matters referred to in paragraph (1): Provided, That this shall not apply where the information collected by the personal information controller does not contain any personal information, such as contact

Question	Assessment Criteria	Enforceability
		information, through which notification can be given to the data subject. <*Newly Inserted on Mar. 29, 2016; Feb. 4, 2020*> (3) Matters necessary for the time, method, and procedure of giving notification to the data subject pursuant to the main clause of paragraph (2), shall be prescribed by Presidential Decree. <*Newly Inserted on Mar. 29, 2016*> (4) Paragraph (1) and the main clause of paragraph (2) shall not apply to any of the following cases: Provided, That this shall be the case only where it is manifestly superior to the rights of data subjects under this Act: <*Amended on Mar. 29, 2016; Mar. 14, 2023*> 1. Where personal information, which is subject to a notification request, is included in the personal information files referred to in any subparagraph of Article 32 (2); 2. Where such notification is likely to cause harm to the life or body of any other person, or to unfairly damage the property and other interests of any other person.
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 Organization 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 Organization to identify: • Each type of data collected;	**Article 3 (Principles of Information Protection)** (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes. (2) The personal information controller shall process personal information in an appropriate manner

Question	Assessment Criteria	Enforceability
	• The corresponding stated purpose of collection for each; • All uses that apply to each type of data; and • 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 Organization limits the amount and type of personal information to that which is relevant to fulfill the stated purposes. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization 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.	necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes. **...** **Article 16 (Restriction on Collection of Personal Information)** (1) A personal information controller shall collect the minimum personal information necessary to attain the purpose when collecting personal information pursuant to Article 15 (1). In such cases, the burden of proof that the minimum personal information is collected shall be borne by the personal information controller. (2) A personal information controller shall collect personal information by specifically informing a data subject of the fact that he or she may deny the consent to the collection of other personal information than the minimum information necessary in case of collecting the personal information with consent of the data subject. *<Newly Inserted on Aug. 6, 2013>* (3) A personal information controller shall not refuse to provide goods or services to a data subject on ground that the data subject does not consent to the collection of personal information exceeding minimum requirement. *<Amended on Aug. 6, 2013>*

Question	Assessment Criteria	Enforceability
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 Organization answers **YES,** the Accountability Agent must require the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform that Applicant Organization that lawful and fair procedures are required for compliance with this Privacy Principle.	**Article 3 (Principles of Information Protection)** (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes. **...**

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 Privacy 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 Organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that Applicant Organization.

Question	Assessment Criteria	Enforceability
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 necessary, provide a description in the space below.	Where the Applicant Organization 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 Organization's privacy statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Organization Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	**Article 15 (Collection and Use of Personal Information)** (1) A personal information controller may collect personal information in any of the following cases, and use it within the scope of the purpose of collection: *<Amended on Mar. 14, 2023>* 1. Where consent is obtained from a data subject; 2. Where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations; 3. Where it is unavoidable for a public institution's performance of work under its jurisdiction as prescribed by statutes or regulations, etc.;

Question	Assessment Criteria	Enforceability
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? 9.b) Compelled by applicable laws?	Where the Applicant Organization answers **NO** to question 8, the Applicant Organization must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the Applicant Organization selects 9a, the Accountability Agent must require the Applicant Organization to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant Organization'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 • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant Organization answers 9.a, the Accountability Agent must require the Applicant Organization to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below.	4. Where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract; 5. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party; 6. Where it is necessary to attain the legitimate interests of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the legitimate interests of the personal information controller and does not go beyond a reasonable scope. 7. Where it is urgently necessary for the public safety and security, public health, etc. ... **Article 18 (Restriction on Repurposing Personal Information and Provision Thereof)** (1) No personal information controller shall use personal information beyond the scope provided in Article 15 (1) or provide it to any third party beyond the scope provided in Articles 17 (1) and 28-8 (1). *<Amended on Feb. 4, 2020; Mar. 14, 2023>* (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information

Question	Assessment Criteria	Enforceability
	Where the Applicant Organization selects 9.b, the Accountability Agent must require the Applicant Organization to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant Organization does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	controller may repurpose personal information or provide it to a third party, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That subparagraphs 5 through 9 shall be applied only to public institutions: <*Amended on Feb. 4, 2020; Mar. 14, 2023*> 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes; 3. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party; 4. Deleted; <*Feb. 4, 2020*> 5. Where it is impossible to perform the work under its jurisdiction as provided in other statutes, unless the personal information controller repurposes personal information or provides it to a third party, and it is subject to the deliberation and resolution by the Commission; 6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention; 7. Where it is necessary for the investigation of a crime, institution and maintenance of a prosecution; 8. Where it is necessary for a court to proceed with trial-related work; 9. Where it is necessary for the enforcement of

Question	Assessment Criteria	Enforceability
		punishment, probation and custody; 10. Where it is urgently necessary for the public safety and security, public health, etc. (3) A personal information controller shall inform the data subject of the following matters when it obtains the consent under paragraph (2) 1; the same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose of use of personal information (in the case of provision of personal information, it means the purpose of use by the recipient); 3. Particulars of personal information to be used or provided; 4. The period for retaining and using personal information (where personal information is provided, it means the period for retention and use by the recipient); 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (4) Where a public institution repurposes personal information or provides it to a third party under paragraph (2) 2 through 6 and 8 through 10, the public institution shall post matters necessary for the legal basis for such use or provision, purpose, scope, and the like on the Official Gazette or on its website, as prescribed by Notification of the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>*

Question	Assessment Criteria	Enforceability
		(5) Where a personal information controller provides personal information to a third party for another purpose in any case provided in any subparagraph of paragraph (2), the personal information controller shall request the recipient of the personal information to limit the purpose and method of use and other necessary matters, or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person upon receipt of such request shall take measures necessary to ensure the safety of the personal information.
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. 11. Do you transfer personal information to personal information processors? If YES, describe.	Where the Applicant Organization 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 Organization to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and	**Article 17 (Provision of Personal Information)** (1) A personal information controller may provide (or share; hereinafter the same shall apply) the personal information of a data subject to a third party in any of the following cases: <*Amended on Feb. 4, 2020; Mar. 14, 2023*> 1. Where consent is obtained from the data subject; 2. Where the personal information is provided within the scope of purposes for which it is collected pursuant to Articles 15 (1) 2, 3, and 5 through 7. (2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose for which the recipient of personal information uses such information;

Question	Assessment Criteria	Enforceability
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.	3) 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 Organization's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	3. Particulars of personal information to be provided; 4. The period during which the recipient retains and uses personal information; 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (3) Deleted. *<Mar. 14, 2023>* (4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether measures necessary to secure safety, such as encryption, have been taken, etc. *<Newly Inserted on Feb. 4, 2020>* **Article 26 (Restriction on Personal Information Processing Subsequent to Entrustment of Work)** (1) A personal information controller shall, when entrusting the processing of personal information to a third party, do so in a document that states the following: *<Amended on Mar. 14, 2023>* 1. Prevention of personal information processing for other purposes than performing the entrusted work; 2. Technical and managerial safeguards of personal information;

Question	Assessment Criteria	Enforceability
		3. Other matters prescribed by Presidential Decree to ensure safe management of personal information. (2) A personal information controller who entrusts the processing of personal information pursuant to paragraph (1) (hereinafter referred to as "person entrusting") shall disclose the details of the entrusted affairs and the entity that processes personal information (including a third party re-entrusted from a person entrusted with the processing of personal information; hereinafter referred to as “person entrusted”) in the manner prescribed by Presidential Decree so as to be easily recognizable by data subjects at any time. *<Amended on Mar. 14, 2023>* (3) The person entrusting shall, in case of entrusting the promotion of goods or services, or soliciting of sales thereof, notify data subjects of the entrusted work and the person entrusted in the manners prescribed by Presidential Decree. The same shall apply where the entrusted work or the person entrusted has been changed. (4) The person entrusting shall educate the person entrusted so that personal information of data subjects may not be lost, stolen, divulged, forged, altered, or damaged owing to the outsourcing of work, and supervise how the person entrusted processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree. *<Amended on Jul. 24, 2015>* (5) An person entrusted shall not use any personal information beyond the scope of the work entrusted by the personal information controller, nor provide personal information to a third party.

Question	Assessment Criteria	Enforceability
		(6) A person entrusted shall, when he or she intends to re-entrust the processing of entrusted personal information to a third party, obtain consent from the person entrusting. *<Newly Inserted on Mar. 14, 2023>* (7) With respect to liability for damages arising out of the processing of personal information entrusted to an person entrusted in violation of this Act, the person entrusted shall be deemed an employee of the personal information controller. *<Amended on Mar. 14, 2023>* (8) Articles 15 through 18, 21, 22, 22-2, 23, 24, 24-2, 25, 25-2, 27, 28, 28-2 through 28-5, 28-7 through 28-11, 29, 30, 30-2, 31, 33, 34, 34-2, 35, 35-2, 36, 37, 37-2, 38, 59, 63, 63-2, and 64-2 shall apply mutatis mutandis to outsourcees. In such cases, "personal information controller" shall be construed as "person entrusted". *<Amended on Mar. 14, 2023>*
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? 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 Applicant Organization answers **NO** to question 13, the Applicant Organization must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant Organization answers **YES** to 13.a, the Accountability Agent must require the Applicant Organization 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;	**Article 18 (Restriction on Repurposing Personal Information and Provision Thereof)** (1) No personal information controller shall use personal information beyond the scope provided in Article 15 (1) or provide it to any third party beyond the scope provided in Articles 17 (1) and 28-8 (1). *<Amended on Feb. 4, 2020; Mar. 14, 2023>* (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may repurpose personal information or provide it to a third party, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That subparagraphs 5 through 9

Question	Assessment Criteria	Enforceability
	• Via e-mail; • Via preference/profile page; • Via telephone; • Via postal mail; or • Other (in case, specify). Where the Applicant Organization answers **YES** to 13.b, the Accountability Agent must require the Applicant Organization 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. Where the Applicant Organization answers **YES** to 13.c, the Accountability Agent must require the Applicant Organization to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant Organization must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant Organization is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement.	shall be applied only to public institutions: <*Amended on Feb. 4, 2020; Mar. 14, 2023*> 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes; 3. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party; 4. Deleted; <*Feb. 4, 2020*> 5. Where it is impossible to perform the work under its jurisdiction as provided in other statutes, unless the personal information controller repurposes personal information or provides it to a third party, and it is subject to the deliberation and resolution by the Commission; 6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention; 7. Where it is necessary for the investigation of a crime, institution and maintenance of a prosecution; 8. Where it is necessary for a court to proceed with trial-related work; 9. Where it is necessary for the enforcement of punishment, probation and custody; 10. Where it is urgently necessary for the public safety and security, public health, etc.

Question	Assessment Criteria	Enforceability
	Where the Applicant Organization answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	(3) A personal information controller shall inform the data subject of the following matters when it obtains the consent under paragraph (2) 1; the same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose of use of personal information (in the case of provision of personal information, it means the purpose of use by the recipient); 3. Particulars of personal information to be used or provided; 4. The period for retaining and using personal information (where personal information is provided, it means the period for retention and use by the recipient); 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (4) Where a public institution repurposes personal information or provides it to a third party under paragraph (2) 2 through 6 and 8 through 10, the public institution shall post matters necessary for the legal basis for such use or provision, purpose, scope, and the like on the Official Gazette or on its website, as prescribed by Notification of the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>* (5) Where a personal information controller provides personal information to a third party for another purpose in any case provided in any subparagraph of paragraph (2), the personal information controller shall request the recipient of the personal information to

Question	Assessment Criteria	Enforceability
		limit the purpose and method of use and other necessary matters, or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person upon receipt of such request shall take measures necessary to ensure the safety of the personal information. **Article 19 (Restriction on Use and Provision of Personal Information on Part of Its Recipients)** A person who receives personal information from a personal information controller shall not use the personal information, or provide it to a third party, for any purpose other than the intended one, except in the following circumstances: 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes. **Article 26 (Restriction on Personal Information Processing Subsequent to Entrustment of Work)** ... (5) An person entrusted shall not use any personal information beyond the scope of the work entrusted by the personal information controller, nor provide personal information to a third party. (6) A person entrusted shall, when he or she intends to re-entrust the processing of entrusted personal information to a third party, obtain consent from the person entrusting. *<Newly Inserted on Mar. 14, 2023>*

Question	Assessment Criteria	Enforceability
		... (8) Articles 15 through 18, 21, 22, 22-2, 23, 24, 24-2, 25, 25-2, 27, 28, 28-2 through 28-5, 28-7 through 28-11, 29, 30, 30-2, 31, 33, 34, 34-2, 35, 35-2, 36, 37, 37-2, 38, 59, 63, 63-2, and 64-2 shall apply mutatis mutandis to outsourcees. In such cases, "personal information controller" shall be construed as "person entrusted". *<Amended on Mar. 14, 2023>*

CHOICE

Assessment Purpose - Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Privacy 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 the Qualifications to the Provision of Choice Mechanisms listed below .

Question	Assessment Criteria	Enforceability
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 purpose of collection is clearly stated.	**Article 15 (Collection and Use of Personal Information)** (1) A personal information controller may collect personal information in any of the following cases, and use it within the scope of the purpose of collection: *<Amended on Mar. 14, 2023>* 1. Where consent is obtained from a data subject; 2. Where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations; 3. Where it is unavoidable for a public institution's performance of work under its jurisdiction as prescribed by statutes or regulations, etc.; 4. Where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract; 5. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party;

Question	Assessment Criteria	Enforceability
	Where the Applicant Organization answers **NO**, the Applicant Organization must identify the applicable Qualification and the Accountability Agent must verify whether the applicable Qualification is justified. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification the Accountability Agent must inform the Applicant Organization that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	6. Where it is necessary to attain the legitimate interests of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the legitimate interests of the personal information controller and does not go beyond a reasonable scope. 7. Where it is urgently necessary for the public safety and security, public health, etc. (2) A personal information controller shall inform a data subject of the following matters when it obtains consent under paragraph (1) 1. The same shall apply when any of the following is modified: 1. The purpose of the collection and use of personal information; 2. Particulars of personal information to be collected; 3. The period for retaining and using personal information; 4. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (3) A personal information controller may use personal information without the consent of a data subject within the scope reasonably related to the initial purpose of the collection as prescribed by Presidential Decree, in consideration whether disadvantages have been caused to the data subject and whether necessary
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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).	

Question	Assessment Criteria	Enforceability
	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 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 Organization answers **NO**, the Applicant Organization 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.	measures to ensure safety such as encryption have been taken. *<Newly Inserted on Feb. 4, 2020>* **Article 37 (Suspension of Processing of Personal Information)** (1) A data subject may request the relevant personal information controller to suspend the processing of his or her personal information or may withdraw his or her consent to personal information processing. In such cases, if the personal information controller is a public institution, the data subject may request the institution to suspend the processing of his or her personal information contained in the personal information files to be registered pursuant to Article 32 or may withdraw his or her consent to personal information processing. *<Amended on Mar. 14, 2023>* (2) Upon receipt of the request for suspension of processing under paragraph (1), the personal information controller shall, without delay, suspend processing of some or all of the personal information as requested by the data subject: Provided, That, where any of the following is applicable, the personal information controller may deny the request of such data subject: *<Amended on Mar. 14, 2023>* 1. Where special provisions exist in other statutes or it is unavoidable to observe obligations under statutes or regulations; 2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person; 3. Where the public institution cannot perform its

Question	Assessment Criteria	Enforceability
	Where the Applicant Organization answers **NO** and does not identify an acceptable Qualification, the Accountability Agent must inform the Applicant Organization a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	work as prescribed by any Act without processing the personal information in question; 4. Where it is impracticable to perform a contract such as the provision of services as agreed upon with the said data subject without processing the personal information in question, and the data subject has not clearly expressed the desire to terminate the agreement. (3) A personal information controller shall, when a data subject withdraws his or her consent pursuant to paragraph (1), take necessary measures without delay, such as destroying collected personal information to prevent recovery and reproduction thereof: Provided, That in cases falling under any subparagraph of paragraph (2), a personal information controller need not take measures following the withdrawal of consent. *<Newly Inserted on Mar. 14, 2023>* (4) When rejecting a request for suspension of processing pursuant to the proviso of paragraph (2) or failing to take measures following the withdrawal of consent pursuant to the proviso of paragraph (3), the personal information controller shall notify the data subject of the reason without delay. *<Amended on Mar. 14, 2023>* (5) 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 requested by data subjects. *<Amended on Mar. 14, 2023>* (6) Matters necessary for the methods and procedures to request the suspension of processing, to withdraw consent, to reject such request, and to give notification,

Question	Assessment Criteria	Enforceability
		etc. pursuant to paragraphs (1) through (5) shall be prescribed by Presidential Decree. <*Amended on Mar. 14, 2023*>
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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. Subject to the Qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:	**Article 17 (Provision of Personal Information)** (1) A personal information controller may provide (or share; hereinafter the same shall apply) the personal information of a data subject to a third party in any of the following cases: <*Amended on Feb. 4, 2020; Mar. 14, 2023*> 1. Where consent is obtained from the data subject; 2. Where the personal information is provided within the scope of purposes for which it is collected pursuant to Articles 15 (1) 2, 3, and 5 through 7. (2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose for which the recipient of personal information uses such information; 3. Particulars of personal information to be provided; 4. The period during which the recipient retains and uses personal information; 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

Question	Assessment Criteria	Enforceability
	• 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 Organization'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 Organization answers **NO**, the Applicant Organization must identify the applicable Qualification and provide a description and the Accountability Agent must verify whether the applicable Qualification is justified. Where the Applicant Organization answers **NO** and does not identify an acceptable Qualification, the Accountability Agent must inform the Applicant Organization that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	(3) Deleted. *<Mar. 14, 2023>* (4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether measures necessary to secure safety, such as encryption, have been taken, etc. *<Newly Inserted on Feb. 4, 2020>* **Article 19 (Restriction on Use and Provision of Personal Information on Part of Its Recipients)** A person who receives personal information from a personal information controller shall not use the personal information, or provide it to a third party, for any purpose other than the intended one, except in the following circumstances: 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes. **Article 37 (Suspension of Processing of Personal Information)** (1) A data subject may request the relevant personal information controller to suspend the processing of his or her personal information or may withdraw his or her consent to personal information processing. In such cases, if the personal information controller is a public

Question	Assessment Criteria	Enforceability
		institution, the data subject may request the institution to suspend the processing of his or her personal information contained in the personal information files to be registered pursuant to Article 32 or may withdraw his or her consent to personal information processing. *<Amended on Mar. 14, 2023>* (2) Upon receipt of the request for suspension of processing under paragraph (1), the personal information controller shall, without delay, suspend processing of some or all of the personal information as requested by the data subject: Provided, That, where any of the following is applicable, the personal information controller may deny the request of such data subject: *<Amended on Mar. 14, 2023>* 1. Where special provisions exist in other statutes or it is unavoidable to observe obligations under statutes or regulations; 2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person; 3. Where the public institution cannot perform its work as prescribed by any Act without processing the personal information in question; 4. Where it is impracticable to perform a contract such as the provision of services as agreed upon with the said data subject without processing the personal information in question, and the data subject has not clearly expressed the desire to terminate the agreement. (3) A personal information controller shall, when a data subject withdraws his or her consent pursuant to

Question	Assessment Criteria	Enforceability
		paragraph (1), take necessary measures without delay, such as destroying collected personal information to prevent recovery and reproduction thereof: Provided, That in cases falling under any subparagraph of paragraph (2), a personal information controller need not take measures following the withdrawal of consent. *<Newly Inserted on Mar. 14, 2023>* (4) When rejecting a request for suspension of processing pursuant to the proviso of paragraph (2) or failing to take measures following the withdrawal of consent pursuant to the proviso of paragraph (3), the personal information controller shall notify the data subject of the reason without delay. *<Amended on Mar. 14, 2023>* (5) 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 requested by data subjects. *<Amended on Mar. 14, 2023>* (6) Matters necessary for the methods and procedures to request the suspension of processing, to withdraw consent, to reject such request, and to give notification, etc. pursuant to paragraphs (1) through (5) shall be prescribed by Presidential Decree. *<Amended on Mar. 14, 2023>*
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	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization's choice mechanism is displayed in a clear and conspicuous manner.	**Article 22 (Methods of Obtaining Consent)** **...** (2) Where a personal information controller obtains the consent under paragraph (1) in writing (including electronic documents under Article 2, subparagraph 1 of the Framework Act on Electronic Documents and Transactions), the personal information controller shall

Question	Assessment Criteria	Enforceability
clear and conspicuous manner?	Where the Applicant Organization answers **NO**, or when the Accountability Agent finds that the Applicant Organization's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	clearly specify important matters prescribed by Presidential Decree such as the purpose of collection and use of personal information and the items of personal information to be collected and used, in the manner prescribed by Notification of the Protection Commission, so as to make such matters easy to be understood. *<Newly Inserted on Apr. 18, 2017; Jul. 26, 2017; Feb. 4, 2020>* (3) With respect to the personal information that can be processed without consent of the data subject, a personal information controller shall disclose the relevant items and legal basis for such processing under Article 30 (2) by separating such information from the personal information processed with consent of the data subject, or shall inform the data subject thereof by e-mail or any other means prescribed by Presidential Decree. In such cases, the burden of proof that personal information can be processed without consent shall be borne by the personal information controller. *<Amended on Mar. 29, 2016; Apr. 18, 2017; Mar. 14, 2023>* (4) Deleted. *<Mar. 14, 2023>* (5) A personal information controller shall not refuse to provide goods or services to a data subject on the grounds that the data subject would not consent to the matter eligible for selective consent, or would not consent pursuant to paragraph (1) 3 and 7. *<Amended on Apr. 18, 2017; Mar. 14, 2023>* (6) Deleted. *<Mar. 14, 2023>* (7) Except as provided in paragraphs (1) through (5), matters necessary for detailed methods to obtain the
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization's choice mechanism is clearly worded and easily understandable. Where the Applicant Organization answers **NO**, and/or when the Accountability Agent finds that the Applicant Organization's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization's choice mechanism is easily accessible and affordable.	

Question	Assessment Criteria	Enforceability
disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant Organization answers **NO**, or when the Accountability Agent finds that the Applicant Organization's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	consent of data subjects shall be prescribed by Presidential Decree, in consideration of the collection media of personal information and other factors. *<Amended on Apr. 18, 2017; Mar. 14, 2023>* **Article 38 (Methods and Procedures for Exercise of Rights)** (1) A data subject may authorize his or her representative to file requests for access under Article 35, transmission under Article 35-2, rectification or erasure under Article 36, suspension of processing and withdrawal of consent under Article 37, and refusal and requests for explanation, etc. under Article 37-2 (hereinafter referred to as "request for access, etc.") by the methods and procedures prescribed by Presidential Decree, such as written documents. *<Amended on Feb. 4, 2020; Mar. 14, 2023>* (2) The legal representative of a child under 14 years of age may file a request for access, etc. to the personal information of the child with a personal information controller. (3) A personal information controller may charge a person who files a request for access, etc. a fee and postage (only in cases of a request to mail the copies), as prescribed by Presidential Decree: Provided, That in cases of a request for transmission under Article 35-2 (2), the personal information controller may assess a fee, taking into account additional facilities necessary for
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 Organization does have mechanisms in place, the Accountability Agent must require the Applicant Organization 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 Organization does not have mechanisms in place, the Applicant Organization 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 Organization answers **NO** and does not provide an acceptable Qualification, the Accountability Agent must inform the Applicant Organization that a mechanism to ensure that choices, when offered, can be honored, must be provided.	

Question	Assessment Criteria	Enforceability
		transmission and other factors as well. <*Amended on Mar. 14, 2023*> (4) A personal information controller shall prepare detailed methods and procedures to enable data subjects to file requests for access, etc., and disclose such methods and procedures so that the data subjects may become aware of them. In such cases, the methods and procedures for filing requests for access, etc. shall be no more difficult than the methods and procedures for the collection of the relevant personal information. <*Amended on Mar. 14, 2023*> (5) A personal information controller shall prepare and provide necessary procedures for data subjects to raise objections regarding the denial of a request for access, etc. from such data subjects.

Qualifications to the Provision of Choice Mechanisms

The following are situations in which the application of the Global CBPR Choice Principle may not be necessary or practical.

i. **Obviousness:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information.

ii. **Collection of Publicly-Available Information**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the collection and use of publicly available information.

iii. **Technological Impracticability**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to those cases where electronic technology automatically collects information when a prospective customer initiates contact [e.g., use of cookies]. However, a mechanism to exercise choice as to use and disclosure should be provided after collection of the information.

iv. **Third-Party Receipt**: Where personal information is received from a third party, the recipient personal information controller does not need to provide a mechanism for individuals to exercise choice in relation to the collection of the information. However, if the personal information controller engages a third party to collect personal information on its behalf, the personal information controller should instruct the collector to provide such choice when collecting the personal information.

v. **Disclosure to a government institution which has made a request for the information with lawful authority**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to disclosure to law enforcement agencies for investigation purposes where the provision of such mechanism to the individual will likely prejudice the investigation.

vi. **Disclosure to a third party pursuant to a lawful form of process:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vii. **For legitimate investigation purposes**: When providing a mechanism for individuals to exercise choice would compromise the availability or accuracy of the personal information and its collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. **Action in the event of an emergency**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in emergency situations that threaten the life, health or security of an individual.

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 Privacy Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.

Question	Assessment Criteria	Enforceability
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use**. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that procedures 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 Privacy Principle.	**Article 3 (Principles of Information Protection)** ... (3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed. ...

Question	Assessment Criteria	Enforceability
22. Do you have a mechanism for correcting inaccurate, incomplete and outdated 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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures and steps the Applicant Organization has in place for correcting inaccurate, incomplete and outdated 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	**Article 36 (Correction or Erasure of Personal Information)** (1) A data subject who has accessed his or her personal information pursuant to Article 35 may request a correction or erasure of such personal information from the relevant personal information controller: Provided, That the erasure is not permitted where the said personal information shall be collected by other statutes or regulations. (2) Upon receipt of a request by a data subject pursuant to paragraph (1), the personal information controller shall investigate the personal information in question without delay; shall take measures necessary to correct or erase as requested by the data subject unless otherwise specifically provided by other statutes or regulations in relation to correction or erasure; and shall notify such data subject of the result. (3) The personal information controller shall take measures not to recover or revive the personal information in case of erasure pursuant to paragraph (2). (4) Where the request of a data subject falls under the proviso of paragraph (1), a personal information controller shall notify the data subject of the details thereof without delay. (5) While investigating the personal information in question pursuant to paragraph (2), the personal information controller may, if necessary, request from the relevant data subject the evidence necessary to confirm a correction or erasure of the personal information. (6) Matters necessary for the request of correction and erasure, notification method and procedure, etc. pursuant to paragraphs (1), (2) and (4) shall be prescribed by Presidential Decree.

Question	Assessment Criteria	Enforceability
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization'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 Organization's behalf. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization 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 Privacy Principle.	**Article 3 (Principles of Information Protection)** ... (3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed. ... **Article 26 (Restriction on Personal Information Processing Subsequent to Entrustment of Work)** (1) A personal information controller shall, when entrusting the processing of personal information to a third party, do so in a document that states the following: *<Amended on Mar. 14, 2023>* 1. Prevention of personal information processing for other purposes than performing the entrusted work; 2. Technical and managerial safeguards of personal information; 3. Other matters prescribed by Presidential Decree to ensure safe management of personal information. (2) A personal information controller who entrusts the processing of personal information pursuant to paragraph (1) (hereinafter referred to as "person entrusting") shall disclose the details of the entrusted affairs and the entity that processes personal information (including a third party re-entrusted from a person entrusted with the processing of personal information; hereinafter referred to as "person entrusted") in the manner prescribed by Presidential

Question	Assessment Criteria	Enforceability
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this Privacy Principle.	Decree so as to be easily recognizable by data subjects at any time. *<Amended on Mar. 14, 2023>* (3) The person entrusting shall, in case of entrusting the promotion of goods or services, or soliciting of sales thereof, notify data subjects of the entrusted work and the person entrusted in the manners prescribed by Presidential Decree. The same shall apply where the entrusted work or the person entrusted has been changed. (4) The person entrusting shall educate the person entrusted so that personal information of data subjects may not be lost, stolen, divulged, forged, altered, or damaged owing to the outsourcing of work, and supervise how the person entrusted processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree. *<Amended on Jul. 24, 2015>* (5) An person entrusted shall not use any personal information beyond the scope of the work entrusted by the personal information controller, nor provide personal information to a third party. (6) A person entrusted shall, when he or she intends to re-entrust the processing of entrusted personal information to a third party, obtain consent from the person entrusting. *<Newly Inserted on Mar. 14, 2023>* (7) With respect to liability for damages arising out of the processing of personal information entrusted to an person entrusted in violation of this Act, the person entrusted shall be deemed an employee of the personal information controller. *<Amended on Mar. 14, 2023>* (8) Articles 15 through 18, 21, 22, 22-2, 23, 24, 24-2,
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 Organization answers **YES**, the Accountability Agent must require the Applicant Organization to provide the procedures the Applicant Organization 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 Organization about any personal information known to be inaccurate incomplete, or outdated.	

Question	Assessment Criteria	Enforceability
	The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant Organization and by the processors, agents or other service providers. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization 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 Privacy principle.	25, 25-2, 27, 28, 28-2 through 28-5, 28-7 through 28-11, 29, 30, 30-2, 31, 33, 34, 34-2, 35, 35-2, 36, 37, 37-2, 38, 59, 63, 63-2, and 64-2 shall apply mutatis mutandis to outsourcees. In such cases, "personal information controller" shall be construed as "person entrusted". *<Amended on Mar. 14, 2023>* **Enforcement Decree of the Personal Information Protection Act** **Article 28 (Measures to be Taken when Entrusting Personal Information Processing))** ... (6) Where a person entrusted processes personal information, the person entrusting shall supervise whether the person entrusting complies with the obligations of a personal information controller provided for in the Act and this Decree and the matters referred to in Article 26 (1) of the Act, pursuant to Article 26 (4) of the Act.

SECURITY SAFEGUARDS

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

Question	Assessment Criteria	Enforceability
26. Have you implemented an information security policy?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that the implementation of a written information security policy is required for compliance with this Privacy Principle.	**Article 29 (Duty of Safeguards)** Every personal information controller shall take such technical, managerial, and physical measures as establishing an internal management plan and preserving access records, etc. that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged. <*Amended on Jul. 24, 2015*> **Enforcement Decree of the Personal Information Protection Act** **Article 30 (Measures to Ensure Safety of Personal Information)** (1) Each personal information controller shall take the following measures to ensure safety pursuant to Article 29 of the Act: <*Amended on Sep. 12, 2023*> 1. Formulating, implementing, and examining an internal management plan that includes the following to safely process personal information: (a) Matters regarding the management, supervision, and education of a personal information handler under Article 28 (1) of the Act (hereinafter referred to as "personal information handler");
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 Organization 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 (e.g., password protections)** • **Encryption** • **Boundary protection (e.g., firewalls, intrusion detection)** • **Audit logging**	

Question	Assessment Criteria	Enforceability
	• **Monitoring (e.g., external and internal audits, vulnerability scans)** • **Other (specify)** The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization'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 Organization 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 Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	(b) Matters regarding the composition and operation of an organization responsible for protecting personal information, including the designation of privacy officers, under Article 31 of the Act; (c) Details necessary to implement the measures provided in subparagraphs 2 through 8; 2. The following measures to restrict access authority to personal information: (a) Establishing and implementing the standards for granting, changing, or canceling access authority to a system systematically designed to process personal information including a database system (hereinafter referred to as "personal information processing system"); (b) Establishing and operating the standards for applying authentication means necessary to verify whether access is made by a person with legitimate authority; (c) Other measures necessary to restrict access authority to personal information; 3. The following measures to control access to personal information: (a) Measures necessary to detect and block intrusions into a personal information processing system; (b) Blocking Internet access to and from computers satisfying the standards determined and publicly notified by the Protection Commission, such as the computers of personal information

Question	Assessment Criteria	Enforceability
	Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.	handlers accessing a personal information processing system: Provided, That this shall apply only to a personal information controller with an average of at least one million daily users defined in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection whose personal information is stored and managed for the immediately preceding three months as of the end of the previous year; (c) Other measures necessary to control access to personal information; 4. The following measures necessary to safely store and transmit personal information: (a) Storing encrypted authentication information, including the storage of one-way encrypted passwords, or other measures equivalent thereto; (b) Encrypting information determined and publicly notified by the Protection Commission for storage, including resident registration numbers, or other measures equivalent thereto; (c) Where the personal information or authentication information of data subjects is transmitted or received through the information and communications network defined in Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, encrypting the relevant information or other measures equivalent thereto; (d) Other measures to ensure security using encryption or other technologies equivalent thereto;
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 Organization 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 Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization'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.	

Question	Assessment Criteria	Enforceability
		5. The following measures to retain the records of access and prevent such records from being forged or altered in case of a personal information breach incident: (a) Storing, inspecting, confirming, and supervising the records of access, such as the date and time when persons access a personal information processing system, and the details of processing personal information; (b) Safely storing the records of access to a personal information processing system; (c) Other measures necessary to retain the records of access and prevent such records from being forged or altered; 6. Installing, operating, and periodically updating and inspecting programs that can detect at all times whether any malicious program, such as a computer virus, spyware, and ransomware, intrudes into a personal information processing system and an information technology equipment used by personal information handlers for processing personal information and that can delete such malicious program; 7. Preparing storage facilities and installing locking devices to safely store personal information, or taking other physical measures; 8. Other measures necessary to ensure safety of personal information. (2) The Protection Commission may provide necessary assistance, such as building a system with which personal information controllers can take the measures to ensure safety pursuant to paragraph (1). *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4. 2020>*

Question	Assessment Criteria	Enforceability
		(3) Detailed standards for the measures to ensure safety under paragraph (1) shall be prescribed by Notification of the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>* **Regulation on Standards for Measures to Ensure the Security of Personal Information** **Article 3 (Principles for Applying Safeguards)** A personal information controller shall apply the necessary measures to ensure the security of personal information, considering the number of personal information records held, the type of personal information, and the impact on data subjects, in a manner appropriate to its own environment.
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 Organization'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, or • Other (specify).	**Article 28 (Supervision of Personal Information Handlers)** (1) In processing personal information, a personal information controller shall limit the scope of persons who process the personal information under his or her command and supervision, such as an executive officer or employee, temporary agency worker, and part-time worker (hereinafter referred to as "personal information handler") to a minimum extent and shall appropriately manage and supervise such personal information handlers. *<Amended on Mar. 14, 2023>* (2) A personal information controller shall provide personal information handlers with necessary educational programs on a regular basis in order to ensure the appropriate handling of personal information.

Question	Assessment Criteria	Enforceability
	Where the Applicant Organization 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 Organization that the existence of such procedures are required for compliance with this Privacy 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 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?	Where the Applicant Organization 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 Organization must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant Organization answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant Organization that the existence of safeguards on each category is required for compliance with this Privacy Principle.	**Article 29 (Duty of Safeguards)** Every personal information controller shall take such technical, managerial, and physical measures as establishing an internal management plan and preserving access records, etc. that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged. *<Amended on Jul. 24, 2015>* **Enforcement Decree of the Personal Information Protection Act** **Article 30 (Measures to Ensure Safety of Personal Information)** (1) Each personal information controller shall take the following measures to ensure safety pursuant to Article 29 of the Act: *<Amended on Sep. 12, 2023>* 1. Formulating, implementing, and examining an internal management plan that includes the following to safely process personal information: (a) Matters regarding the management, supervision, and education of a personal information handler under Article 28 (1) of the Act (hereinafter

Question	Assessment Criteria	Enforceability
		referred to as "personal information handler"); (b) Matters regarding the composition and operation of an organization responsible for protecting personal information, including the designation of privacy officers, under Article 31 of the Act; (c) Details necessary to implement the measures provided in subparagraphs 2 through 8; 2. The following measures to restrict access authority to personal information: (a) Establishing and implementing the standards for granting, changing, or canceling access authority to a system systematically designed to process personal information including a database system (hereinafter referred to as "personal information processing system"); (b) Establishing and operating the standards for applying authentication means necessary to verify whether access is made by a person with legitimate authority; (c) Other measures necessary to restrict access authority to personal information; 3. The following measures to control access to personal information: (a) Measures necessary to detect and block intrusions into a personal information processing system; (b) Blocking Internet access to and from computers satisfying the standards determined and publicly notified by the Protection Commission, such as the

Question	Assessment Criteria	Enforceability
		computers of personal information handlers accessing a personal information processing system: Provided, That this shall apply only to a personal information controller with an average of at least one million daily users defined in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection whose personal information is stored and managed for the immediately preceding three months as of the end of the previous year; (c) Other measures necessary to control access to personal information; 4. The following measures necessary to safely store and transmit personal information: (a) Storing encrypted authentication information, including the storage of one-way encrypted passwords, or other measures equivalent thereto; (b) Encrypting information determined and publicly notified by the Protection Commission for storage, including resident registration numbers, or other measures equivalent thereto; (c) Where the personal information or authentication information of data subjects is transmitted or received through the information and communications network defined in Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, encrypting the relevant information or other measures equivalent thereto; (d) Other measures to ensure security using encryption or other technologies equivalent thereto;

Question	Assessment Criteria	Enforceability
		5. The following measures to retain the records of access and prevent such records from being forged or altered in case of a personal information breach incident: (a) Storing, inspecting, confirming, and supervising the records of access, such as the date and time when persons access a personal information processing system, and the details of processing personal information; (b) Safely storing the records of access to a personal information processing system; (c) Other measures necessary to retain the records of access and prevent such records from being forged or altered; 6. Installing, operating, and periodically updating and inspecting programs that can detect at all times whether any malicious program, such as a computer virus, spyware, and ransomware, intrudes into a personal information processing system and an information technology equipment used by personal information handlers for processing personal information and that can delete such malicious program; 7. Preparing storage facilities and installing locking devices to safely store personal information, or taking other physical measures; 8. Other measures necessary to ensure safety of personal information. (2) The Protection Commission may provide necessary assistance, such as building a system with which personal information controllers can take the measures to ensure safety pursuant to paragraph (1). *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4. 2020>*

Question	Assessment Criteria	Enforceability
		(3) Detailed standards for the measures to ensure safety under paragraph (1) shall be prescribed by Notification of the Protection Commission. <*Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020*> **Regulation on Standards for Measures to Ensure the Security of Personal Information** **Article 3 (Principles for Applying Safeguards)** A personal information controller shall apply the necessary measures to ensure the security of personal information, considering the number of personal information records held, the type of personal information, and the impact on data subjects, in a manner appropriate to its own environment.
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant Organization answers **NO**, the Accountability Agent must inform Applicant Organization that the existence of a policy for the secure disposal of personal information is required for compliance with this Privacy Principle.	**Article 21 (Destruction of Personal Information)** (1) A personal information controller shall destroy personal information without delay when the personal information becomes unnecessary owing to the expiry of the retention period, attainment of the purpose of processing the personal information, the expiry of the processing period of pseudonymized information, etc.: Provided, That this shall not apply where the retention of such personal information is mandatory by other statutes or regulations. <*Amended on Mar. 14, 2023*>

Question	Assessment Criteria	Enforceability
		(2) When a personal information controller destroys personal information pursuant to paragraph (1), measures necessary to prevent recovery and revival shall be taken. (3) Where a personal information controller is obliged to retain, rather than destroy, personal information pursuant to the provison of paragraph (1), the relevant personal information or personal information files shall be stored and managed separately from other personal information. (4) Other necessary matters, such as the methods to destroy personal information and its destruction process, shall be prescribed by Presidential Decree.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant Organization 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 Organization answers **NO,** the Accountability Agent must inform the Applicant Organization that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this Privacy Principle.	**Article 29 (Duty of Safeguards)** Every personal information controller shall take such technical, managerial, and physical measures as establishing an internal management plan and preserving access records, etc. that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged. *<Amended on Jul. 24, 2015>* **Enforcement Decree of the Personal Information Protection Act** **Article 30 (Measures to Ensure Safety of Personal Information)** (1) Each personal information controller shall take the following measures to ensure safety pursuant to Article 29 of the Act: *<Amended on Sep. 12, 2023>*

Question	Assessment Criteria	Enforceability
		1. Formulating, implementing, and examining an internal management plan that includes the following to safely process personal information: (a) Matters regarding the management, supervision, and education of a personal information handler under Article 28 (1) of the Act (hereinafter referred to as "personal information handler"); (b) Matters regarding the composition and operation of an organization responsible for protecting personal information, including the designation of privacy officers, under Article 31 of the Act; (c) Details necessary to implement the measures provided in subparagraphs 2 through 8; 2. The following measures to restrict access authority to personal information: (a) Establishing and implementing the standards for granting, changing, or canceling access authority to a system systematically designed to process personal information including a database system (hereinafter referred to as "personal information processing system"); (b) Establishing and operating the standards for applying authentication means necessary to verify whether access is made by a person with legitimate authority; (c) Other measures necessary to restrict access authority to personal information; 3. The following measures to control access to personal information:
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 Organization adjusts their security safeguards to reflect the results of these tests.	

Question	Assessment Criteria	Enforceability
		(a) Measures necessary to detect and block intrusions into a personal information processing system; (b) Blocking Internet access to and from computers satisfying the standards determined and publicly notified by the Protection Commission, such as the computers of personal information handlers accessing a personal information processing system: Provided, That this shall apply only to a personal information controller with an average of at least one million daily users defined in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection whose personal information is stored and managed for the immediately preceding three months as of the end of the previous year; (c) Other measures necessary to control access to personal information; 4. The following measures necessary to safely store and transmit personal information: (a) Storing encrypted authentication information, including the storage of one-way encrypted passwords, or other measures equivalent thereto; (b) Encrypting information determined and publicly notified by the Protection Commission for storage, including resident registration numbers, or other measures equivalent thereto; (c) Where the personal information or authentication information of data subjects is transmitted or received through the information and communications network defined in Article 2 (1) 1 of the Act on Promotion of Information
34. Do you use **third- party certifications or other risk assessments**? Describe below.	The Accountability Agent must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant Organization 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 Organization and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	

Question	Assessment Criteria	Enforceability
		and Communications Network Utilization and Information Protection, encrypting the relevant information or other measures equivalent thereto; (d) Other measures to ensure security using encryption or other technologies equivalent thereto; 5. The following measures to retain the records of access and prevent such records from being forged or altered in case of a personal information breach incident: (a) Storing, inspecting, confirming, and supervising the records of access, such as the date and time when persons access a personal information processing system, and the details of processing personal information; (b) Safely storing the records of access to a personal information processing system; (c) Other measures necessary to retain the records of access and prevent such records from being forged or altered; 6. Installing, operating, and periodically updating and inspecting programs that can detect at all times whether any malicious program, such as a computer virus, spyware, and ransomware, intrudes into a personal information processing system and an information technology equipment used by personal information handlers for processing personal information and that can delete such malicious program; 7. Preparing storage facilities and installing locking devices to safely store personal information, or taking other physical measures; 8. Other measures necessary to ensure safety of personal information.

Question	Assessment Criteria	Enforceability
		(2) The Protection Commission may provide necessary assistance, such as building a system with which personal information controllers can take the measures to ensure safety pursuant to paragraph (1). *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4. 2020>* (3) Detailed standards for the measures to ensure safety under paragraph (1) shall be prescribed by Notification of the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>* **<u>Regulation on Standards for Measures to Ensure the Security of Personal Information</u>** **Article 4 (Establishment, Implementation, and Inspection of Internal Management Plans)** (1) A personal information controller shall establish and implement an internal management plan, through internal decision-making procedures, so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged. Such plan shall include the matters listed in the following subparagraphs. However, this may be omitted for small business owners, individuals, or organizations processing personal information fewer than 10,000 data subjects. ... 13. Matters concerning risk analysis and management ... **Article 32-2 (Certification of Personal Information Protection)** **Article 33 (Privacy Impact Assessment)**

Question	Assessment Criteria	Enforceability
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, 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 Organization's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	The Accountability Agent must verify that the Applicant Organization 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 Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	**Article 26 (Restriction on Personal Information Processing Subsequent to Entrustment of Work)** (1) A personal information controller shall, when entrusting the processing of personal information to a third party, do so in a document that states the following: *<Amended on Mar. 14, 2023>* 1. Prevention of personal information processing for other purposes than performing the entrusted work; 2. Technical and managerial safeguards of personal information; 3. Other matters prescribed by Presidential Decree to ensure safe management of personal information. (2) A personal information controller who entrusts the processing of personal information pursuant to paragraph (1) (hereinafter referred to as "person entrusting") shall disclose the details of the entrusted affairs and the entity that processes personal information (including a third party re-entrusted from a person entrusted with the processing of personal information; hereinafter referred to as "person entrusted") in the manner prescribed by Presidential Decree so as to be easily recognizable by data subjects at any time. *<Amended on Mar. 14, 2023>* (3) The person entrusting shall, in case of entrusting the promotion of goods or services, or soliciting of sales thereof, notify data subjects of the entrusted work and the person entrusted in the manners prescribed by Presidential Decree. The same shall apply where the entrusted work or the person entrusted has been changed.

Question	Assessment Criteria	Enforceability
		(4) The person entrusting shall educate the person entrusted so that personal information of data subjects may not be lost, stolen, divulged, forged, altered, or damaged owing to the outsourcing of work, and supervise how the person entrusted processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree. *<Amended on Jul. 24, 2015>* (5) An person entrusted shall not use any personal information beyond the scope of the work entrusted by the personal information controller, nor provide personal information to a third party. (6) A person entrusted shall, when he or she intends to re-entrust the processing of entrusted personal information to a third party, obtain consent from the person entrusting. *<Newly Inserted on Mar. 14, 2023>* (7) With respect to liability for damages arising out of the processing of personal information entrusted to an person entrusted in violation of this Act, the person entrusted shall be deemed an employee of the personal information controller. *<Amended on Mar. 14, 2023>* (8) Articles 15 through 18, 21, 22, 22-2, 23, 24, 24-2, 25, 25-2, 27, 28, 28-2 through 28-5, 28-7 through 28-11, 29, 30, 30-2, 31, 33, 34, 34-2, 35, 35-2, 36, 37, 37-2, 38, 59, 63, 63-2, and 64-2 shall apply mutatis mutandis to outsourcees. In such cases, "personal information controller" shall be construed as "person entrusted". *<Amended on Mar. 14, 2023>*

ACCESS AND CORRECTION

Assessment Purpose - T*he 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. The Qualifications to the Provision of Access and Correction Mechanisms are listed below and set 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
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has procedures in place to respond to such requests.	**Article 35 (Access to Personal Information)** (1) A data subject may request access to his or her own personal information, which is processed by a personal information controller, from the personal information controller. (2) Notwithstanding paragraph (1), where a data subject

Question	Assessment Criteria	Enforceability
	The Applicant Organization 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 Organization'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 Organization must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	intends to request access to his or her own personal information from a public institution, the data subject may request such access directly from the said public institution, or indirectly via the Protection Commission, as prescribed by Presidential Decree. <*Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020*> (3) Upon receipt of a request for access filed under paragraphs (1) and (2), a personal information controller shall grant the data subject access to his or her own personal information within the period prescribed by Presidential Decree. In such cases, if there is good cause for not permitting access during such period, the personal information controller may postpone access after notifying the relevant data subject of the said ground and if the said ground ceases to exist, the data subject shall be permitted to access the personal information without delay. (4) In any of the following cases, a personal information controller may limit or deny access after it notifies a data subject of the cause: 1. Where access is prohibited or limited by statutes; 2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person; 3. Where a public institution has grave difficulties in performing any of the following work: (a) Imposition, collection or refund of taxes; (b) Evaluation of academic achievements or admission affairs at the schools of each level established under the Elementary and Secondary

Question	Assessment Criteria	Enforceability
		Education Act and the Higher Education Act, lifelong educational facilities established under the Lifelong Education Act, and other higher educational institutions established under other statutes; (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; (e) Ongoing audit and examination under other statutes. (5) Matters necessary for the methods and procedures to file access requests, to limit access, to give notification, etc. pursuant to paragraphs (1) through (4) shall be prescribed by Presidential Decree. **Article 38 (Methods and Procedures for Exercise of Rights)** (1) A data subject may authorize his or her representative to file requests for access under Article 35, transmission under Article 35-2, rectification or erasure under Article 36, suspension of processing and withdrawal of consent under Article 37, and refusal and requests for explanation, etc. under Article 37-2 (hereinafter referred to as "request for access, etc.") by the methods and procedures prescribed by Presidential Decree, such as written documents. <*Amended on Feb. 4, 2020; Mar. 14, 2023*> (2) The legal representative of a child under 14 years of age may file a request for access, etc. to the
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 Organization'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.	Where the Applicant Organization answers **YES,** the Accountability Agent must verify each answer provided. The Applicant Organization 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 Organization 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.	

Question	Assessment Criteria	Enforceability
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.)? 37.e) Do you charge a fee for providing access? If YES, describe below what the fee is based and how you ensure that the fee is not excessive.	Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that it may be required to permit access by individuals to their personal information. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	personal information of the child with a personal information controller. (3) A personal information controller may charge a person who files a request for access, etc. a fee and postage (only in cases of a request to mail the copies), as prescribed by Presidential Decree: Provided, That in cases of a request for transmission under Article 35-2 (2), the personal information controller may assess a fee, taking into account additional facilities necessary for transmission and other factors as well. *<Amended on Mar. 14, 2023>* (4) A personal information controller shall prepare detailed methods and procedures to enable data subjects to file requests for access, etc., and disclose such methods and procedures so that the data subjects may become aware of them. In such cases, the methods and procedures for filing requests for access, etc. shall be no more difficult than the methods and procedures for the collection of the relevant personal information. *<Amended on Mar. 14, 2023>* (5) A personal information controller shall prepare and provide necessary procedures for data subjects to raise objections regarding the denial of a request for access, etc. from such data subjects.
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 Organization's	Where the Applicant Organization answers **YES to questions 38(a)**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy.	**Article 36 (Correction or Erasure of Personal Information)** (1) A data subject who has accessed his or her personal information pursuant to Article 35 may request a correction or erasure of such personal information from the relevant personal information controller: Provided, That the erasure is not permitted where the

Question	Assessment Criteria	Enforceability
policies/procedures in this regard below and answer questions 38 (a) – (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 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?	If the Applicant Organization 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 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 Organization answers **NO** to questions 38(a) – (e) and does not identify an applicable Qualification, the Accountability Agent must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the Accountability Agent must verify whether the applicable Qualification is justified.	said personal information shall be collected by other statutes or regulations. (2) Upon receipt of a request by a data subject pursuant to paragraph (1), the personal information controller shall investigate the personal information in question without delay; shall take measures necessary to correct or erase as requested by the data subject unless otherwise specifically provided by other statutes or regulations in relation to correction or erasure; and shall notify such data subject of the result. (3) The personal information controller shall take measures not to recover or revive the personal information in case of erasure pursuant to paragraph (2). (4) Where the request of a data subject falls under the proviso of paragraph (1), a personal information controller shall notify the data subject of the details thereof without delay. (5) While investigating the personal information in question pursuant to paragraph (2), the personal information controller may, if necessary, request from the relevant data subject the evidence necessary to confirm a correction or erasure of the personal information. (6) Matters necessary for the request of correction and erasure, notification method and procedure, etc. pursuant to paragraphs (1), (2) and (4) shall be prescribed by Presidential Decree. **Article 38 (Methods and Procedures for Exercise of Rights)** (1) A data subject may authorize his or her representative to file requests for access under Article 35, transmission under Article 35-2, rectification or

Question	Assessment Criteria	Enforceability
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?		erasure under Article 36, suspension of processing and withdrawal of consent under Article 37, and refusal and requests for explanation, etc. under Article 37-2 (hereinafter referred to as "request for access, etc.") by the methods and procedures prescribed by Presidential Decree, such as written documents. <*Amended on Feb. 4, 2020; Mar. 14, 2023*> (2) The legal representative of a child under 14 years of age may file a request for access, etc. to the personal information of the child with a personal information controller. (3) A personal information controller may charge a person who files a request for access, etc. a fee and postage (only in cases of a request to mail the copies), as prescribed by Presidential Decree: Provided, That in cases of a request for transmission under Article 35-2 (2), the personal information controller may assess a fee, taking into account additional facilities necessary for transmission and other factors as well. <*Amended on Mar. 14, 2023*> (4) A personal information controller shall prepare detailed methods and procedures to enable data subjects to file requests for access, etc., and disclose such methods and procedures so that the data subjects may become aware of them. In such cases, the methods and procedures for filing requests for access, etc. shall be no more difficult than the methods and procedures for the collection of the relevant personal information. <*Amended on Mar. 14, 2023*> (5) A personal information controller shall prepare and provide necessary procedures for data subjects to raise objections regarding the denial of a request for access, etc. from such data subjects.

Qualifications to the Provision of Access and Correction Mechanisms

Although organizations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organizations to deny access requests. Please identify which, if any, of these situations apply, and specify their application to you, with reference to your responses provided to the previous questions, in the space provided.

i. **Disproportionate Burden:** Personal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.

ii. **Protection of Confidential Information:** Personal information controllers do not need to provide access and correction where the information cannot be disclosed due to legal or security reasons or to protect confidential commercial information (i.e., information that you have taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against your business interest causing significant financial loss). Where confidential commercial information can be readily separated from other information subject to an access request, the personal information controller should redact the confidential commercial information and make available the non-confidential commercial information to the extent that such information constitutes personal information of the individual concerned.

Other situations would include those where disclosure of information would benefit a competitor in the market place, such as a particular computer or modeling program. Furthermore, a denial of access may also be considered acceptable in situations where, for example providing the information would constitute a violation of laws or would compromise security.

iii. **Third Party Risk:** Personal information controllers do not need to provide access and correction where the information privacy of persons other than the individual would be violated. In those instances where a third party's personal information can be severed from the information requested for access or correction, the personal information controller must release the information after redaction of the third party's personal information.

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant Organization is accountable for complying with measures that give effect to the other Privacy Principles stated above. Additionally, when transferring information, the Applicant Organization should be accountable for ensuring that the recipient will protect the information consistently with these Privacy Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Privacy 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 Privacy 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
39. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____	The Accountability Agent has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles.	**Article 29 (Duty of Safeguards)** Every personal information controller shall take such technical, managerial, and physical measures as establishing an internal management plan and preserving access records, etc. that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged. <*Amended on Jul. 24, 2015*>

Question	Assessment Criteria	Enforceability
• Compliance with self-regulatory Applicant Organization code and/or rules ___ • Other (describe) _____		
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Global CBPR Privacy Principles?	Where the Applicant Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization has designated an employee(s) who is responsible for the Applicant Organization's overall compliance with these Privacy Principles. The Applicant Organization must designate an individual or individuals to be responsible for the Applicant Organization'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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that designation of such an employee(s) is required for compliance with this Privacy Principle.	**Article 31 (Designation of Privacy Officers)** (1) A personal information controller shall designate a privacy officer who shall have general supervision and control of the work regarding personal information processing: Provided, That a personal information controller whose number of employees, turnover, etc. meet the criteria prescribed by Presidential Decree need not designate a privacy officer. *<Amended on Mar. 14, 2023>* (2) Where a privacy officer is not designated under the proviso of paragraph (1), the business owner or representative of the personal information controller shall become the privacy officer. *<Newly Inserted on Mar. 14, 2023>* (3) A privacy officer shall perform the following work: *<Amended on Mar. 14, 2023>* 1. To establish and implement a personal information protection plan; 2. To conduct a regular survey of the status and practices of personal information processing, and to improve shortcomings; 3. To handle grievances and remedial compensation in relation to personal information processing;

Question	Assessment Criteria	Enforceability
		4. To build the internal control system to prevent the divulgence, abuse, and misuse of personal information; 5. To prepare and implement an education program about personal information protection; 6. To protect, control, and manage the personal information files; 7. Other work prescribed by Presidential Decree for the appropriate processing of personal information. (4) In performing the work provided in the subparagraphs of paragraph (3), a privacy officer may occasionally inspect the current status of personal information processing, processing systems, etc. if necessary, and may request a report thereon from the relevant parties. <*Amended on Mar. 14, 2023*> (5) Where a privacy officer becomes aware of any violation of this Act or other relevant statutes or regulations in relation to the protection of personal information, he or she shall take corrective measures immediately, and shall report such corrective measures to the head of the institution or organization to which he or she belongs, if necessary. <*Amended on Mar. 14, 2023*> (6) A personal information controller shall not allow the privacy officer to give or be subject to disadvantages without good cause while performing the affairs provided in the subparagraphs of paragraph (3), and shall guarantee the independent performance of work by the privacy officer. <*Amended on Mar. 14, 2023*>

Question	Assessment Criteria	Enforceability
		(7) A personal information controller may organize and operate a council of privacy officers comprised of the privacy officers provided in paragraph (1) so as to safely process and protect personal information, exchange information, and conduct other joint projects prescribed by Presidential Decree. *<Newly Inserted on Mar. 14, 2023>* (8) The Protection Commission may provide support necessary for the activities of the council of privacy officers under paragraph (7). *<Newly Inserted on Mar. 14, 2023>* (9) Matters necessary for the qualification requirements for a privacy officer under paragraph (1), the work under paragraph (3), the guarantee of independence under paragraph (6), and other relevant matters, shall be prescribed by Presidential Decree, taking into consideration sales, the scale of personal information retained, etc. *<Amended on Mar. 14, 2023>*
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization 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 Organization (e.g., Email/Phone/Fax/Postal Mail/Online Form); AND/OR	**Article 30 (Establishment and Disclosure of Privacy Policy)** (1) A personal information controller shall establish a personal information processing policy including the following matters (hereinafter referred to as "Privacy Policy"). In such cases, public institutions shall establish the Privacy Policy for the personal information files to be registered pursuant to Article 32: *<Amended on Mar. 29, 2016; Feb. 4, 2020; Mar. 14, 2023>* ... 6. Contact information, such as the name of a privacy officer designated under Article 31 or the

Question	Assessment Criteria	Enforceability
	2) A designated employee(s) to handle complaints related to the Applicant Organization's compliance with the Global CBPR 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	name, telephone number, etc. of the department which performs the work related to personal information protection and handles related grievances; ... **Article 31 (Designation of Privacy Officers)** ... (3) A privacy officer shall perform the following work: *<Amended on Mar. 14, 2023>* ... 3. To handle grievances and remedial compensation in relation to personal information processing; ...
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	
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 Organization indicates what remedial action is considered.	

Question	Assessment Criteria	Enforceability
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant Organization 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 Organization that the existence of such procedures is required for compliance with this Privacy Principle.	**Article 28 (Supervision of Personal Information Handlers)** (1) In processing personal information, a personal information controller shall limit the scope of persons who process the personal information under his or her command and supervision, such as an executive officer or employee, temporary agency worker, and part-time worker (hereinafter referred to as "personal information handler") to a minimum extent and shall appropriately manage and supervise such personal information handlers. *<Amended on Mar. 14, 2023>* (2) A personal information controller shall provide personal information handlers with necessary educational programs on a regular basis in order to ensure the appropriate handling of personal information.
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 Organization answers **YES,** the Accountability Agent must verify that the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.	**Article 17 (Provision of Personal Information)** (1) A personal information controller may provide (or share; hereinafter the same shall apply) the personal information of a data subject to a third party in any of the following cases: *<Amended on Feb. 4, 2020; Mar. 14, 2023>* 1. Where consent is obtained from the data subject; 2. Where the personal information is provided within the scope of purposes for which it is collected pursuant to Articles 15 (1) 2, 3, and 5 through 7. (2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified:

Question	Assessment Criteria	Enforceability
		1. The recipient of personal information; 2. The purpose for which the recipient of personal information uses such information; 3. Particulars of personal information to be provided; 4. The period during which the recipient retains and uses personal information; 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (3) Deleted. *<Mar. 14, 2023>* (4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether measures necessary to secure safety, such as encryption, have been taken, etc. *<Newly Inserted on Feb. 4, 2020>* **Article 18 (Restriction on Repurposing Personal Information and Provision Thereof)** (1) No personal information controller shall use personal information beyond the scope provided in Article 15 (1) or provide it to any third party beyond the scope provided in Articles 17 (1) and 28-8 (1). *<Amended on Feb. 4, 2020; Mar. 14, 2023>*

Question	Assessment Criteria	Enforceability
		(2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may repurpose personal information or provide it to a third party, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That subparagraphs 5 through 9 shall be applied only to public institutions: <*Amended on Feb. 4, 2020; Mar. 14, 2023*> 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes; 3. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party; 4. Deleted; <*Feb. 4, 2020*> 5. Where it is impossible to perform the work under its jurisdiction as provided in other statutes, unless the personal information controller repurposes personal information or provides it to a third party, and it is subject to the deliberation and resolution by the Commission; 6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention; 7. Where it is necessary for the investigation of a crime, institution and maintenance of a prosecution; 8. Where it is necessary for a court to proceed with trial-related work;

Question	Assessment Criteria	Enforceability
		9. Where it is necessary for the enforcement of punishment, probation and custody; 10. Where it is urgently necessary for the public safety and security, public health, etc. (3) A personal information controller shall inform the data subject of the following matters when it obtains the consent under paragraph (2) 1; the same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose of use of personal information (in the case of provision of personal information, it means the purpose of use by the recipient); 3. Particulars of personal information to be used or provided; 4. The period for retaining and using personal information (where personal information is provided, it means the period for retention and use by the recipient); 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (4) Where a public institution repurposes personal information or provides it to a third party under paragraph (2) 2 through 6 and 8 through 10, the public institution shall post matters necessary for the legal basis for such use or provision, purpose, scope, and the like on the Official Gazette or on its website, as prescribed by Notification of the Protection Commission. *<Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023>*

Question	Assessment Criteria	Enforceability
		(5) Where a personal information controller provides personal information to a third party for another purpose in any case provided in any subparagraph of paragraph (2), the personal information controller shall request the recipient of the personal information to limit the purpose and method of use and other necessary matters, or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person upon receipt of such request shall take measures necessary to ensure the safety of the personal information. **Article 19 (Restriction on Use and Provision of Personal Information on Part of Its Recipients)** A person who receives personal information from a personal information controller shall not use the personal information, or provide it to a third party, for any purpose other than the intended one, except in the following circumstances: 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes. The Act on Anti-Terrorism for the Protection of Citizens and Public Security, the Protection of Communications Secrets Act, the Telecommunications Business Act, the Act on Reporting and Using Specified Financial Transaction Information, the Act on Prohibition of Funds for Terrorism, the Framework Act on National Taxes, the Monopoly Regulation and Fair Trade Act, etc. are strictly protecting the privacy and personal information of owners

Question	Assessment Criteria	Enforceability
		of information by strictly prescribing the requirements and procedures for national agencies' collecting personal information without the consent of the data subject.
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 Organization code and/or rules _____ _ • Others (describe) _____	Where the Applicant Organization answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such agreements is required for compliance with this Privacy Principle.	**Article 26 (Restriction on Personal Information Processing Subsequent to Entrustment of Work)** (1) A personal information controller shall, when entrusting the processing of personal information to a third party, do so in a document that states the following: *<Amended on Mar. 14, 2023>* 1. Prevention of personal information processing for other purposes than performing the entrusted work; 2. Technical and managerial safeguards of personal information; 3. Other matters prescribed by Presidential Decree to ensure safe management of personal information. (2) A personal information controller who entrusts the processing of personal information pursuant to paragraph (1) (hereinafter referred to as "person entrusting") shall disclose the details of the entrusted affairs and the entity that processes personal information (including a third party re-entrusted from a person entrusted with the processing of personal information; hereinafter referred to as "person entrusted") in the manner prescribed by Presidential Decree so as to be easily recognizable by data subjects at any time. *<Amended on Mar. 14, 2023>* (3) The person entrusting shall, in case of entrusting the promotion of goods or services, or soliciting of sales thereof, notify data subjects of the entrusted work and the person entrusted in the manners prescribed by
47. Do these agreements generally require that personal information processors, agents, contractors or other service	The Accountability Agent must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met.	

Question	Assessment Criteria	Enforceability
providers: • Abide by your Global CBPR- 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? _____ • Impose restrictions on subcontracting unless with your consent? _____ • Be Global CBPR-certified by a Forum-recognized Accountability Agent in their jurisdiction? _____ • Notify the Applicant Organization in the case of a breach of the personal information of the Applicant Organization's customers? • Other (describe) ____		Presidential Decree. The same shall apply where the entrusted work or the person entrusted has been changed. (4) The person entrusting shall educate the person entrusted so that personal information of data subjects may not be lost, stolen, divulged, forged, altered, or damaged owing to the outsourcing of work, and supervise how the person entrusted processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree. <*Amended on Jul. 24, 2015*> (5) An person entrusted shall not use any personal information beyond the scope of the work entrusted by the personal information controller, nor provide personal information to a third party. (6) A person entrusted shall, when he or she intends to re-entrust the processing of entrusted personal information to a third party, obtain consent from the person entrusting. <*Newly Inserted on Mar. 14, 2023*> (7) With respect to liability for damages arising out of the processing of personal information entrusted to an person entrusted in violation of this Act, the person entrusted shall be deemed an employee of the personal information controller. <*Amended on Mar. 14, 2023*> (8) Articles 15 through 18, 21, 22, 22-2, 23, 24, 24-2, 25, 25-2, 27, 28, 28-2 through 28-5, 28-7 through 28-11, 29, 30, 30-2, 31, 33, 34, 34-2, 35, 35-2, 36, 37, 37-2, 38, 59, 63, 63-2, and 64-2 shall apply mutatis mutandis to outsourcees. In such cases, "personal information controller" shall be construed as "person entrusted". <*Amended on Mar. 14, 2023*>

Question	Assessment Criteria	Enforceability
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.	
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 Organization answers **YES**, the Accountability Agent must verify the existence of the Applicant Organization's procedures such as spot checking or monitoring mechanisms. Where the Applicant Organization answers **NO**, the Accountability Agent must require the Applicant Organization to describe why it does not make use of such spot checking or monitoring mechanisms.	

Question	Assessment Criteria	Enforceability
50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence and reasonable steps to ensure compliance with the Global CBPR System by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant Organization 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 Organization for ensuring that the information, nevertheless, is protected consistent with the Global CBPR Privacy Principles. Where the Applicant Organization relies on an individual's consent, the Applicant Organization must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	**Article 18 (Restriction on Repurposing Personal Information and Provision Thereof)** (1) No personal information controller shall use personal information beyond the scope provided in Article 15 (1) or provide it to any third party beyond the scope provided in Articles 17 (1) and 28-8 (1). *<Amended on Feb. 4, 2020; Mar. 14, 2023>* (2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may repurpose personal information or provide it to a third party, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That subparagraphs 5 through 9 shall be applied only to public institutions: *<Amended on Feb. 4, 2020; Mar. 14, 2023>* 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes; 3. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party; 4. Deleted; *<Feb. 4, 2020>* 5. Where it is impossible to perform the work under its jurisdiction as provided in other statutes, unless the personal information controller repurposes personal information or provides it to a third party, and it is subject to the deliberation and resolution by the Commission;

Question	Assessment Criteria	Enforceability
		6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention; 7. Where it is necessary for the investigation of a crime, institution and maintenance of a prosecution; 8. Where it is necessary for a court to proceed with trial-related work; 9. Where it is necessary for the enforcement of punishment, probation and custody; 10. Where it is urgently necessary for the public safety and security, public health, etc. (3) A personal information controller shall inform the data subject of the following matters when it obtains the consent under paragraph (2) 1; the same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose of use of personal information (in the case of provision of personal information, it means the purpose of use by the recipient); 3. Particulars of personal information to be used or provided; 4. The period for retaining and using personal information (where personal information is provided, it means the period for retention and use by the recipient); 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

Question	Assessment Criteria	Enforceability
		(4) Where a public institution repurposes personal information or provides it to a third party under paragraph (2) 2 through 6 and 8 through 10, the public institution shall post matters necessary for the legal basis for such use or provision, purpose, scope, and the like on the Official Gazette or on its website, as prescribed by Notification of the Protection Commission. <*Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Feb. 4, 2020; Mar. 14, 2023*> (5) Where a personal information controller provides personal information to a third party for another purpose in any case provided in any subparagraph of paragraph (2), the personal information controller shall request the recipient of the personal information to limit the purpose and method of use and other necessary matters, or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person upon receipt of such request shall take measures necessary to ensure the safety of the personal information. **Article 19 (Restriction on Use and Provision of Personal Information on Part of Its Recipients)** A person who receives personal information from a personal information controller shall not use the personal information, or provide it to a third party, for any purpose other than the intended one, except in the following circumstances: 1. Where separate consent is obtained from the data subject; 2. Where special provisions exist in other statutes.